JOINT APPENDIX
VOLUME III

EXHIBIT 178

Chainalysis

February 2022

The 2022 Crypto Crime Report

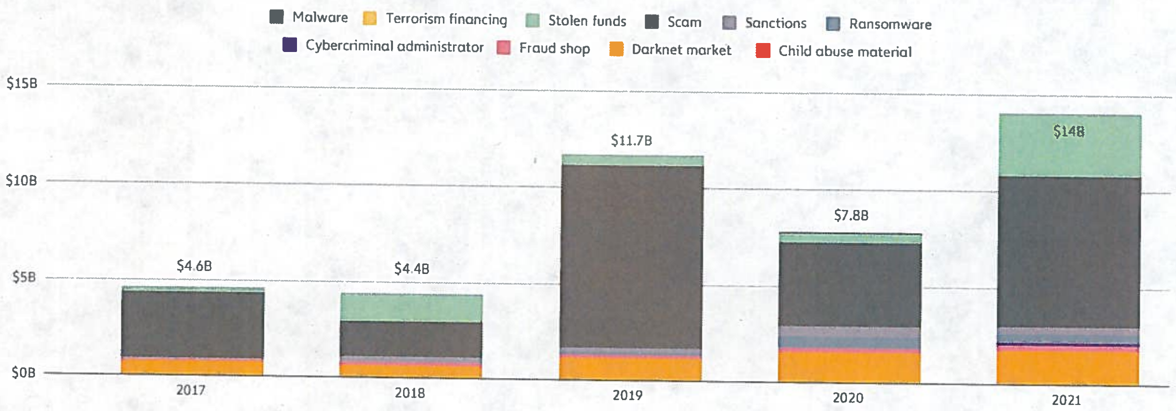
Original data and research into cryptocurrency-based crime

Introduction

Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-time Low in Share of All Cryptocurrency Activity

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020.

Total cryptocurrency value received by illicit addresses | 2017–2021

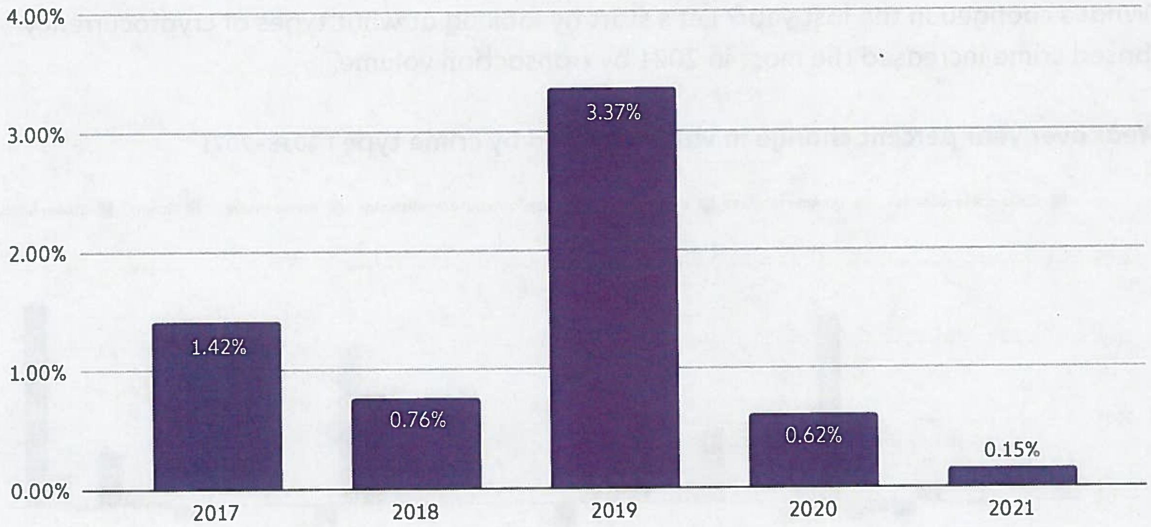


Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

But those numbers don't tell the full story. Cryptocurrency usage is growing faster than ever before. Across all cryptocurrencies tracked by Chainalysis, total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals. Given that roaring adoption, it's no surprise that more cybercriminals are using cryptocurrency. But the fact that the increase in illicit transaction volume was just 79% — nearly an order of magnitude lower than overall adoption — might be the biggest surprise of all.

In fact, with the growth of legitimate cryptocurrency usage far outpacing the growth of criminal usage, illicit activity's share of cryptocurrency transaction volume has never been lower.

Illicit share of all cryptocurrency transaction volume | 2017–2021



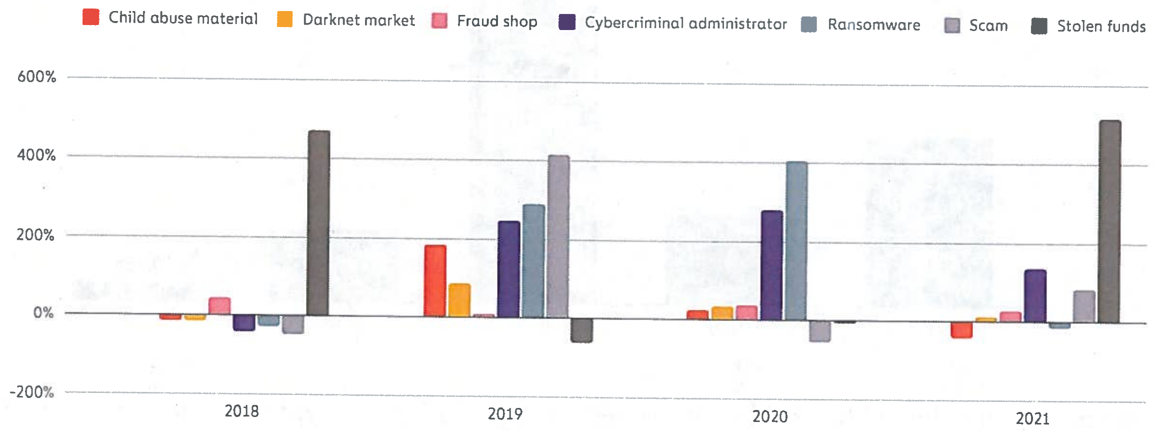
Transactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever. As always, we have to caveat this figure and say that it is likely to rise as Chainalysis identifies more addresses associated with illicit activity and incorporates their transaction activity into our historical volumes. For instance, we found in our last Crypto Crime Report that 0.34% of 2020's cryptocurrency transaction volume was associated with illicit activity — we've now raised that figure to 0.62%. Still, the yearly trends suggest that with the exception of 2019 — an extreme outlier year for cryptocurrency-based crime largely due to the PlusToken Ponzi scheme — crime is becoming a smaller and smaller part of the cryptocurrency ecosystem. Law enforcement's ability to combat cryptocurrency-based crime is also evolving. We've seen several examples of this throughout 2021, from the CFTC filing charges against several investment scams, to the FBI's takedown of the prolific REvil ransomware strain, to OFAC's sanctioning of Suex and Chatex, two Russia-based cryptocurrency services heavily involved in money laundering.

However, we also have to balance the positives of the growth of legal cryptocurrency usage with the understanding that $14 billion worth of illicit activity represents a significant problem. Criminal abuse of cryptocurrency creates huge impediments for continued adoption, heightens the likelihood of restrictions being imposed by governments, and worst of all victimizes innocent people around the world. In this report, we'll explain exactly how and where cryptocurrency-based crime increased, dive into the latest trends amongst different types of cybercriminals, and tell you how cryptocurrency businesses and law enforcement agencies around the world are responding. But first, let's look at a few of the key trends in cryptocurrency-based crime.

DeFi's rise leads to new opportunities in crypto crime

What's changed in the last year? Let's start by looking at what types of cryptocurrency-based crime increased the most in 2021 by transaction volume.

Year over year percent change in value received by crime type | 2018–2021



Two categories stand out for their growth: stolen funds and, to a lesser degree, scams. DeFi is a big part of the story for both.

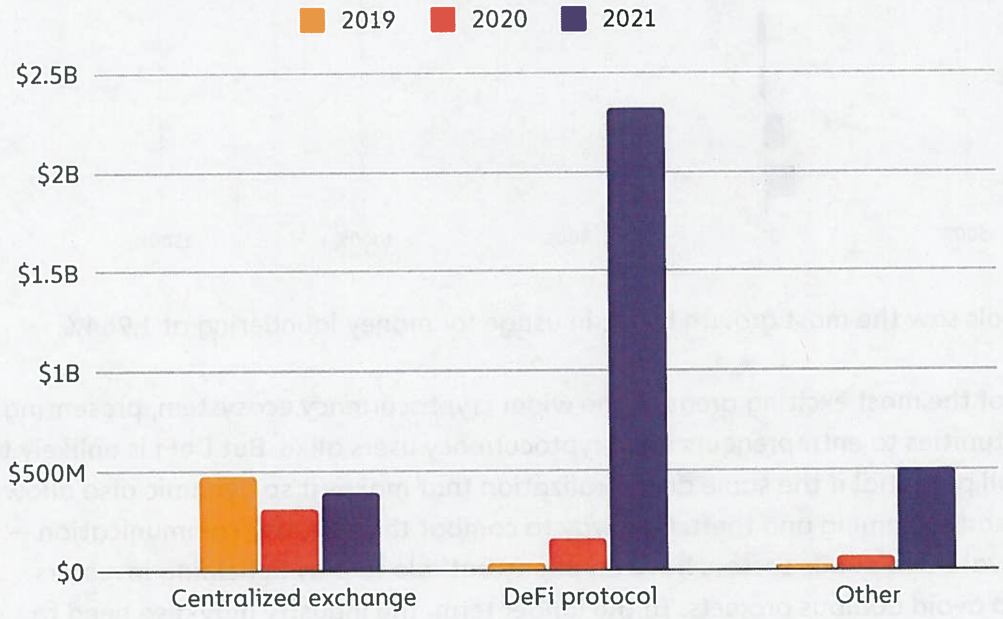
Let's start with scams. Scamming revenue rose 82% in 2021 to $7.8 billion worth of cryptocurrency stolen from victims. Over $2.8 billion of this total — which is nearly equal to the increase over 2020's total — came from rug pulls, a relatively new scam type in which developers build what appear to be legitimate cryptocurrency projects — meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investing opportunities — before taking investors' money and disappearing. Please keep in mind as well that these figures for rug pull losses represent only the value of investors' funds that were stolen, and not losses from the DeFi tokens' subsequent loss of value following a rug pull.

We should note that roughly 90% of the total value lost to rug pulls in 2021 can be attributed to one fraudulent centralized exchange, Thodex, whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. However, every other rug pull tracked by Chainalysis in 2021 involved DeFi projects. In nearly all of these cases, developers have tricked investors into purchasing tokens associated with a DeFi project before draining the tools provided by those investors, sending the token's value to zero in the process.

We believe rug pulls are common in DeFi for two related reasons. One is the hype around the space. DeFi transaction volume has grown 912% in 2021, and the incredible returns on decentralized tokens like Shiba Inu have many excited to speculate on DeFi tokens. At the same time, it's very easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit. A code audit is a process by which a third-party firm or listing exchange analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are iron clad and contain no mechanisms that would allow for the developers to make off with investors' funds. Many investors could likely have avoided losing funds to rug pulls if they'd stuck to DeFi projects that have undergone a code audit – or if DEXes required code audits before listing tokens.

Cryptocurrency theft grew even more, with roughly $3.2 billion worth of cryptocurrency stolen in 2021 — a 516% increase compared to 2020. Roughly $2.2 billion of those funds — 72% of the 2021 total — were stolen from DeFi protocols. The increase in DeFi-related thefts represents the acceleration of a trend we identified in last year's Crypto Crime report.

Annual total cryptocurrency stolen by victim type | JAN '19–DEC '21

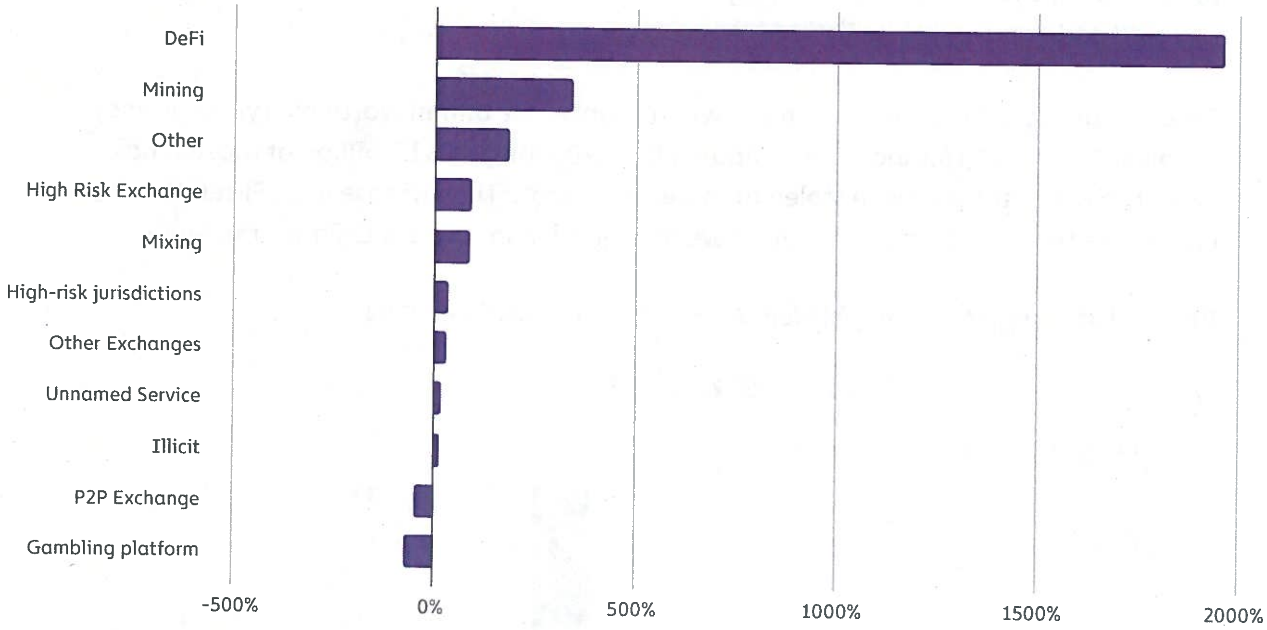


In 2020, just under $162 million worth of cryptocurrency was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. As we'll explore in more detail later in the report, most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur.

We've also seen significant growth in the usage of DeFi protocols for laundering illicit funds, a practice we saw scattered examples of in 2020 and that became more prevalent in 2021. Check out the graph below, which looks at the growth in illicit funds received by different types of services in 2021 compared to 2020.

Year over year percentage growth in value received by service from illicit addresses

2020–2021



DeFi protocols saw the most growth by far in usage for money laundering at 1,964%.

DeFi is one of the most exciting areas of the wider cryptocurrency ecosystem, presenting huge opportunities to entrepreneurs and cryptocurrency users alike. But DeFi is unlikely to realize its full potential if the same decentralization that makes it so dynamic also allows for widespread scamming and theft. One way to combat this is better communication — both the private and public sectors have an important role to play in helping investors learn how to avoid dubious projects. In the longer term, the industry may also need to take more drastic steps to prevent tokens associated with potentially fraudulent or unsafe projects from being listed on major exchanges.

Illicit cryptocurrency balances are growing. What can law enforcement do?

One promising development in the fight against cryptocurrency-related crime is the growing ability of law enforcement to seize illicitly obtained cryptocurrency. In November

2021, for instance, the IRS Criminal Investigations announced that it had seized over $3.5 billion worth of cryptocurrency in 2021 — all from non-tax investigations — representing 93% of all funds seized by the division during that time period. We've also seen several examples of successful seizures by other agencies, including $56 million seized by the Department of Justice in a cryptocurrency scam investigation, $2.3 million seized from the ransomware group behind the Colonial Pipeline attack, and an undisclosed amount seized by Israel's National Bureau for Counter Terror Financing in a case related to terrorism financing.

This raises an interesting question: How much cryptocurrency are criminals currently holding? It's impossible to know for sure, but we can estimate based on the current holdings of addresses Chainalysis has identified as associated with illicit activity. As of early 2022, illicit addresses hold at least $10 billion worth of cryptocurrency, with the vast majority of this held by wallets associated with cryptocurrency theft. Addresses associated with darknet markets and with scams also contribute significantly to this figure. As we'll explore later in this report, much of this value comes not from the initial amount derived from criminal activity, but from subsequent price increases of the crypto assets held.

We believe it's important for law enforcement agencies to understand these estimates as they build out their blockchain-based investigative capabilities, and especially as they develop their ability to seize illicit cryptocurrency.

Let's make cryptocurrency safer

DeFi-related crime and criminal cryptocurrency balances are just one area of focus for this report. We'll also look at the latest data and trends on other forms of cryptocurrency-based crime, including:

- The ongoing threat of ransomware
- Cryptocurrency-based money laundering
- Nation state actors' role in cryptocurrency-based crime
- Illicit activity in NFTs

  And much more!

As cryptocurrency continues to grow, it's imperative that the public and private sectors work together to ensure that users can transact safely, and that criminals can't abuse these new assets. We hope that this report can contribute to that goal, and equip law enforcement, regulators, and compliance professionals with the knowledge to more effectively prevent, mitigate, and investigate cryptocurrency-based crime.

Money Laundering

DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate

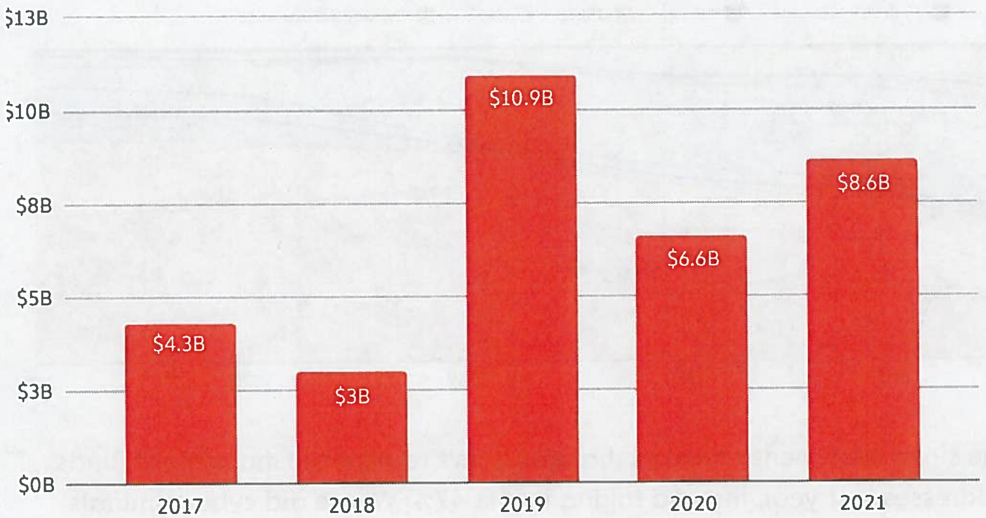
Cybercriminals dealing in cryptocurrency share one common goal: Move their ill-gotten funds to a service where they can be kept safe from the authorities and eventually converted to cash. That's why money laundering underpins all other forms of cryptocurrency-based crime. If there's no way to access the funds, there's no incentive to commit crimes involving cryptocurrency in the first place.

Money laundering activity in cryptocurrency is also heavily concentrated. While billions of dollars' worth of cryptocurrency moves from illicit addresses every year, most of it ends up at a surprisingly small group of services, many of which appear purpose-built for money laundering based on their transaction histories. Law enforcement can strike a huge blow against cryptocurrency-based crime and significantly hamper criminals' ability to access their digital assets by disrupting these services. We saw an example of this last year, when the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned two of the worst-offending money laundering services — Suex and Chatex — for accepting funds from ransomware operators, scammers, and other cybercriminals. But as we'll explore below, many other money laundering services remain active.

2021 cryptocurrency money laundering activity summarized

Overall, going by the amount of cryptocurrency sent from illicit addresses to addresses hosted by services, cybercriminals laundered $8.6 billion worth of cryptocurrency in 2021.

Total cryptocurrency value laundered by year | 2017–2021

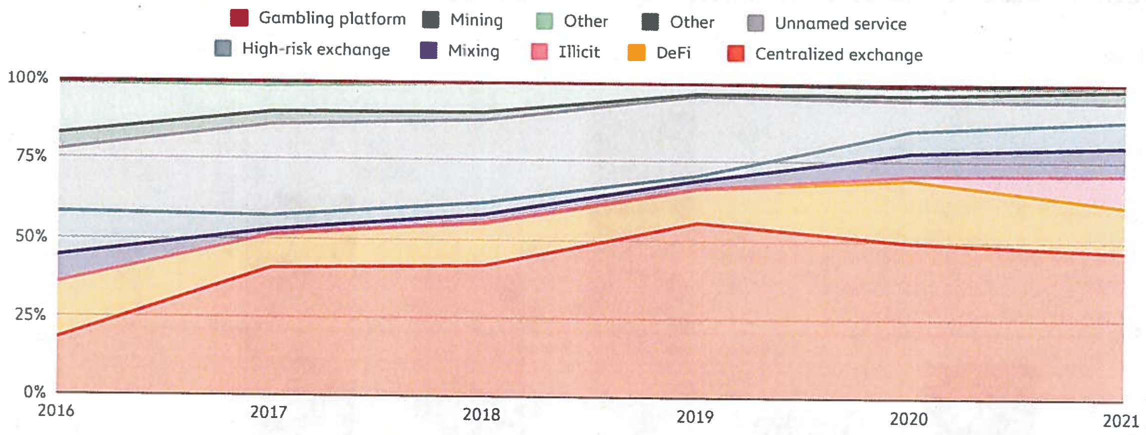


That represents a 30% increase in money laundering activity over 2020, though such an increase is unsurprising given the significant growth of both legitimate and illicit cryptocurrency activity in 2021. We also need to note that these numbers only account for funds derived from "cryptocurrency-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency rather than fiat currency. It's more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into cryptocurrency to be laundered. However, we know anecdotally this is happening, and later in this section provide a case study showing an example of it.

Overall, cybercriminals have laundered over $33 billion worth of cryptocurrency since 2017, with most of the total over time moving to centralized exchanges. For comparison, the UN Office of Drugs and Crime estimates that between $800 billion and $2 trillion of fiat currency is laundered each year — as much as 5% of global GDP. For comparison, money laundering accounted for just 0.05% of all cryptocurrency transaction volume in 2021. We cite those numbers not to try and minimize cryptocurrency's crime-related issues, but rather to point out that money laundering is a plague on virtually all forms of economic value transfer, and to help law enforcement and compliance professionals be aware of just how much money laundering activity could theoretically move to cryptocurrency as adoption of the technology increases.

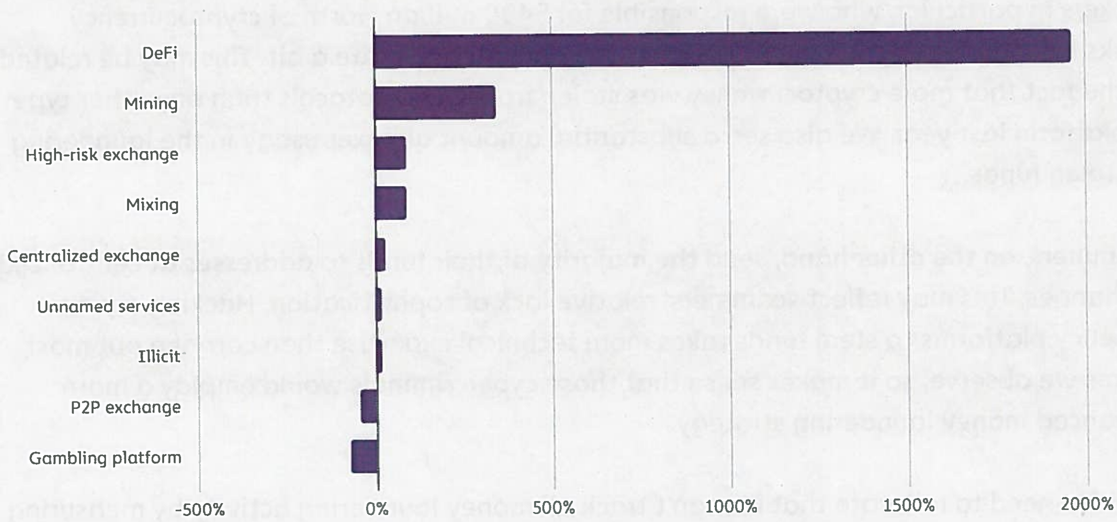
The biggest difference between fiat and cryptocurrency-based money laundering is that, due to the inherent transparency of blockchains, we can more easily trace how criminals move cryptocurrency between wallets and services in their efforts to convert their funds into cash. What kinds of cryptocurrency services do criminals rely on for this?

Destination of funds leaving illicit addresses | 2016–2021



For the first time since 2018, centralized exchanges didn't receive the majority of funds sent by illicit addresses last year, instead taking in just 47%. Where did cybercriminals send funds instead? DeFi protocols make up much of the difference. DeFi protocols received 17% of all funds sent from illicit wallets in 2021, up from 2% the previous year.

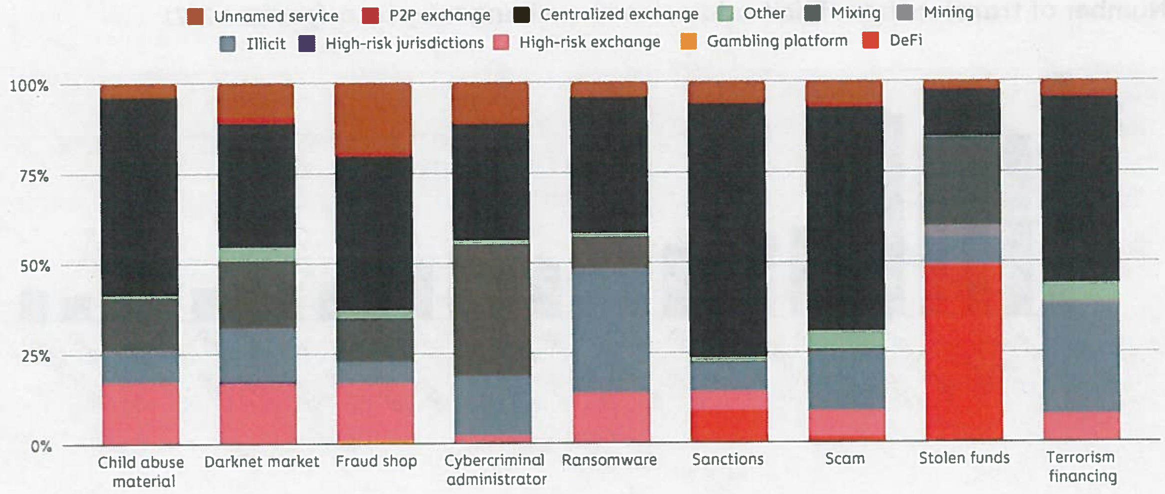
Year over year percentage growth in value received from illicit addresses by service category | 2020–2021



That translates to a 1,964% year-over-year increase in total value received by DeFi protocols from illicit addresses, reaching a total of $900 million in 2021. Mining pools, high-risk exchanges, and mixers also saw substantial increases in value received from illicit addresses as well.

We also see patterns in which types of services different types of cybercriminals use to launder cryptocurrency.

Destination of funds leaving illicit addresses by crime type | 2021



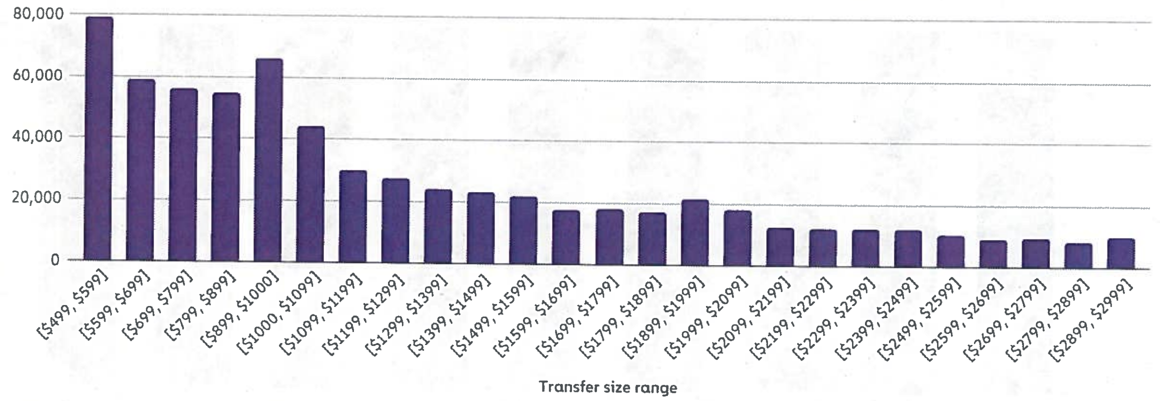
One thing that stands out is the difference in laundering strategies between the two highest-grossing forms of cryptocurrency-based crime in 2021: Theft and scamming.

Addresses associated with theft sent just under half of their stolen funds to DeFi platforms — over $750 million worth of cryptocurrency in total. North Korea-affiliated hackers in particular, who were responsible for $400 million worth of cryptocurrency hacks last year, used DeFi protocols for money laundering quite a bit. This may be related to the fact that more cryptocurrency was stolen from DeFi protocols than any other type of platform last year. We also see a substantial amount of mixer usage in the laundering of stolen funds.

Scammers, on the other hand, send the majority of their funds to addresses at centralized exchanges. This may reflect scammers' relative lack of sophistication. Hacking cryptocurrency platforms to steal funds takes more technical expertise than carrying out most scams we observe, so it makes sense that those cybercriminals would employ a more advanced money laundering strategy.

We also need to reiterate that we can't track all money laundering activity by measuring the value sent from known criminal addresses. As stated above, some criminals use cryptocurrency to launder funds from crimes that happen offline, and there are many criminal addresses in use that have yet to be identified. However, we can account for some of these more obscured instances of money laundering by looking for transaction patterns suggesting that users were trying to avoid compliance screens. For instance, due to regulations like the Travel Rule, cryptocurrency businesses in many countries must conduct additional compliance checks, reporting, and information sharing related to transactions above $1,000 USD in value. As you might expect, illicit addresses send a disproportionate number of transfers to exchanges just below that $1,000 threshold.

Number of transfers from illicit addresses to exchanges by transfer size | 2021

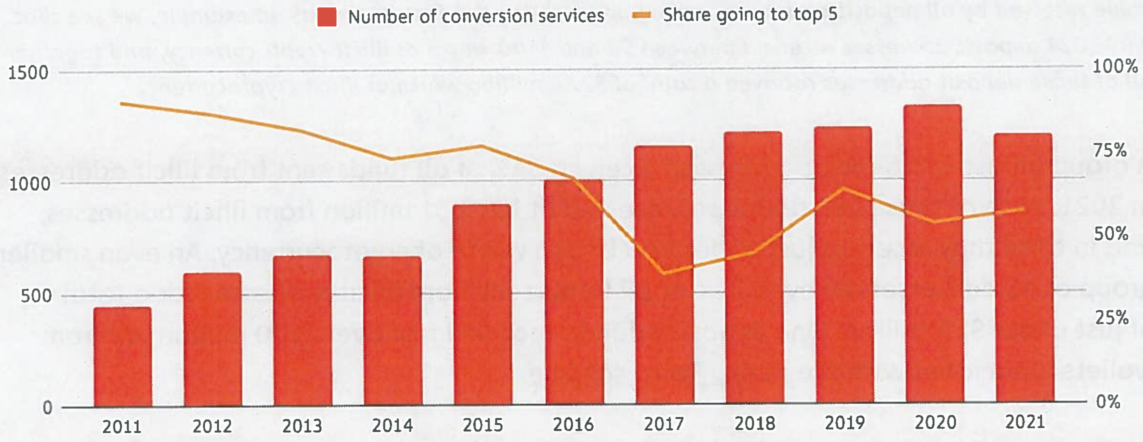


Exchanges using Chainalysis would be able to see that these funds are coming from illicit addresses regardless of transfer size. But more generally, compliance teams should consider treating users who consistently send or receive transactions of that size with extra scrutiny. Repeated instances of transactions just below the threshold may indicate users are doing what's known as structuring, meaning purposely breaking up large payments into smaller ones just below reporting thresholds in order to fool compliance teams.

Money laundering activity remains highly concentrated in 2021, but less so than in 2020

As we've discussed previously, money laundering activity is heavily concentrated to just a few services. We can see how that concentration has changed over time below.

Share of illicit cryptocurrency moving to top five services and total number of unique services receiving illicit cryptocurrency | 2011–2021

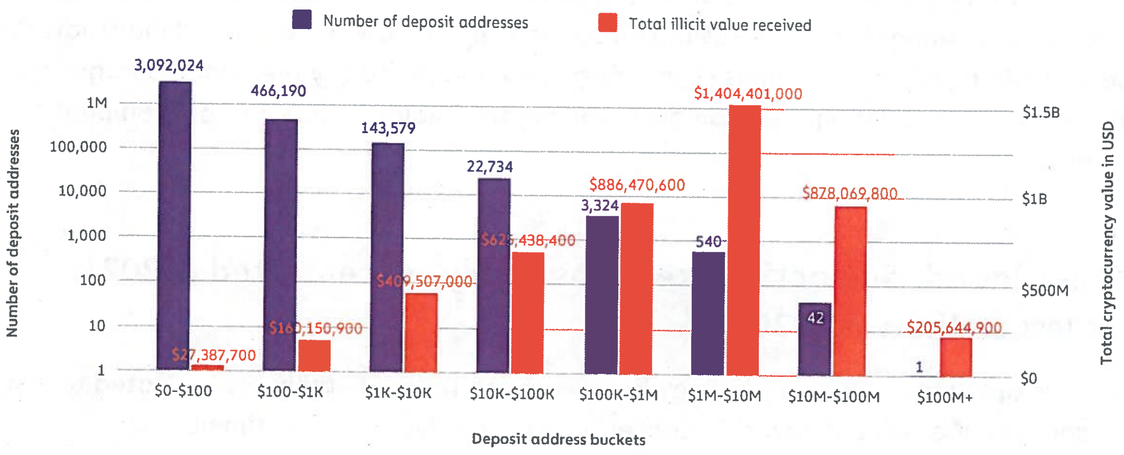


With fewer services used in 2021, money laundering concentration initially appears to have increased slightly. 58% of all funds sent from illicit addresses moved to five services last year, compared to 54% in 2020.

However, money laundering activity is better viewed at the deposit address level rather than the service level. The reason for that is that many of the money laundering services used by cybercriminals are nested services, meaning they operate using addresses hosted by larger services in order to tap into those larger services' liquidity and trading pairs. Over-the-counter (OTC) brokers, for example, often function as nested services with addresses hosted by large exchanges. In the graph below, we look at all service deposit addresses that received any illicit funds in 2021, broken down by the range of illicit funds received.

All illicit cryptocurrency received by service deposit addresses

Deposit addresses bucketed by total illicit cryptocurrency received | 2021



How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency value each address received individually in 2021. Each blue bar represents the number of deposit addresses in the bucket, while each orange bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 3,092,024 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $27.4 million worth of illicit cryptocurrency.

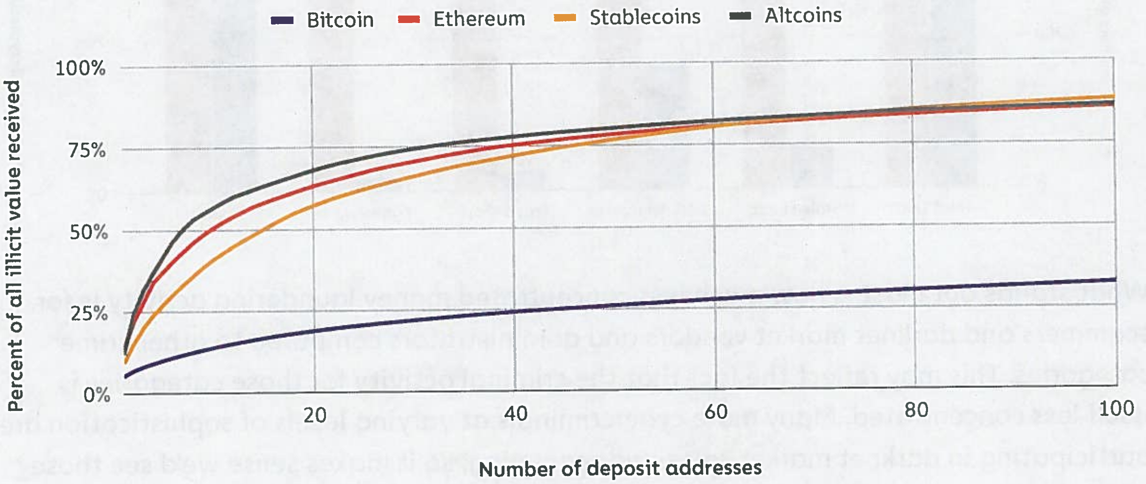
A group of just 583 deposit addresses received 54% of all funds sent from illicit addresses in 2021. Each of those 583 addresses received at least $1 million from illicit addresses, and in total they received just under $2.5 billion worth of cryptocurrency. An even smaller group of 45 addresses received 24% of all funds sent from illicit addresses for a total of just under $1.1 billion. One deposit address received just over $200 million, all from wallets associated with the Finiko Ponzi scheme.

While money laundering activity remains quite concentrated, it's less so than in 2020. That year, 55% of all cryptocurrency sent from illicit addresses went to just 270 service deposit addresses. Law enforcement action could be one possible reason money laundering activity became less concentrated. As we mentioned above, last year OFAC sanctioned Suex, a Russia-based OTC broker, that had received tens of millions' of dollars' worth of cryptocurrency from addresses associated with ransomware, scams, and other forms of criminal activity. Soon after, OFAC also sanctioned Chatex, a P2P exchange founded by the same person as Suex with a similar client profile. While we couldn't share their names at the time, addresses associated with both services appeared in the 270 we identified as the biggest laundering addresses in last year's report.

It's possible that some money laundering services ceased operations after seeing those and other actions taken against illicit platforms, forcing cybercriminals to disperse their money laundering activity to other operators. It's also possible that money laundering services have continued to operate but spread their activity across more deposit addresses, which would contribute to the lessening concentration we see above.

We also see differing levels of concentration in money laundering depending on the asset.

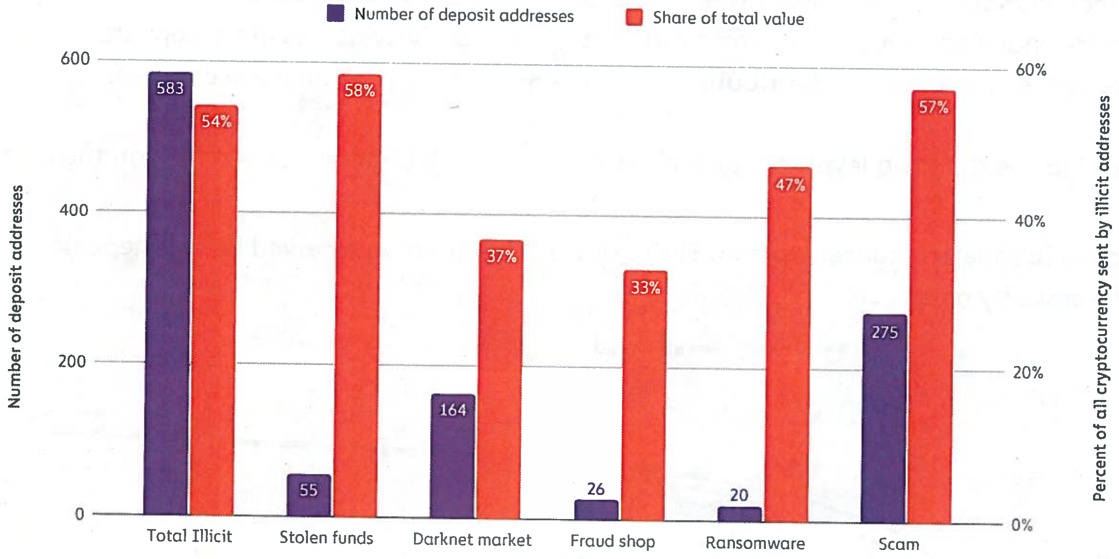
Money laundering concentration: Share of total illicit value received by top deposit addresses by asset | 2021



Bitcoin's money laundering activity is the least concentrated by far. The 20 biggest money laundering deposit addresses receive just 19% of all Bitcoin sent from illicit addresses, compared to 57% for stablecoins, 63% for Ethereum, and 68% for altcoins.

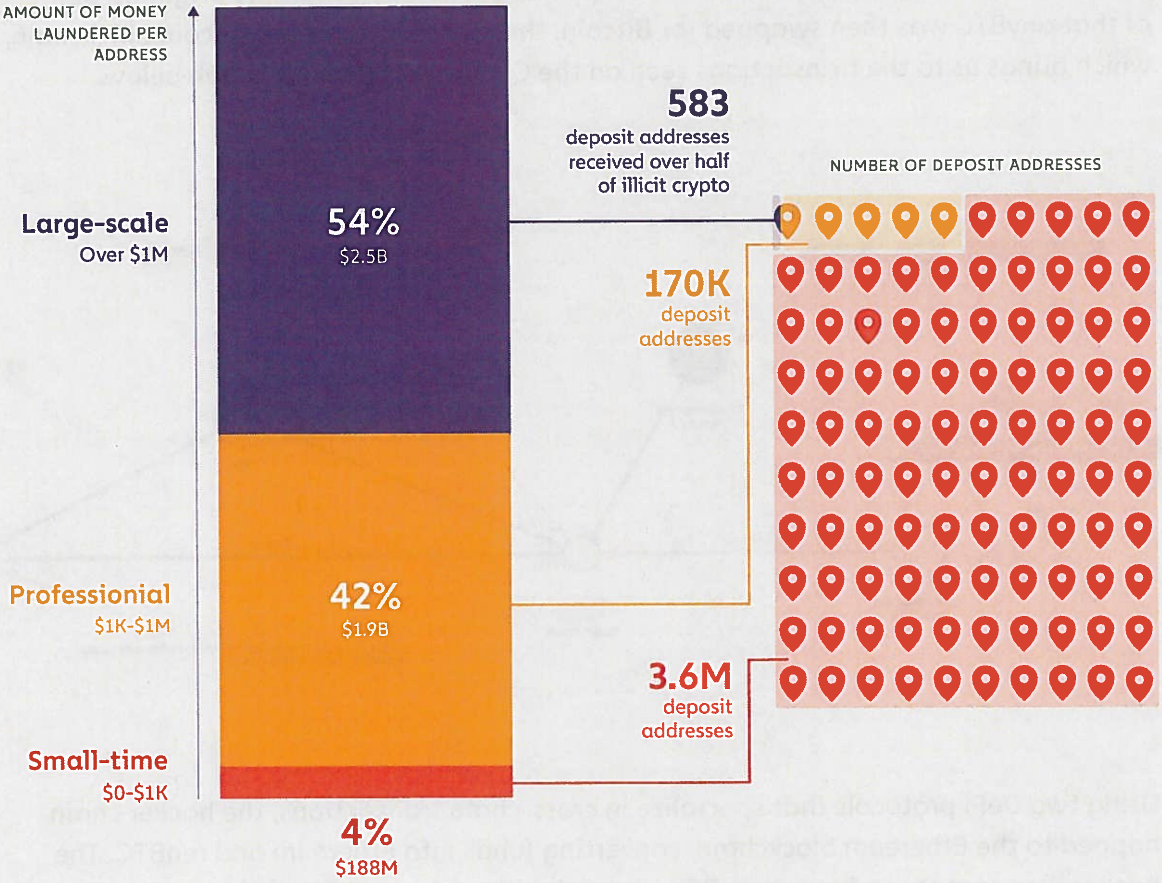
We also see differences in the level of money laundering concentration for different types of cybercriminals. The chart below breaks down by crime category all addresses that received over $1 million in illicit cryptocurrency in 2021, and the share of all funds sent from those criminal categories that the deposit addresses account for.

Number of deposit addresses receiving over $1M in illicit cryptocurrency by crime category and share of all value sent by crime category | 2021



What stands out most is how much less concentrated money laundering activity is for scammers and darknet market vendors and administrators compared to other crime categories. This may reflect the fact that the criminal activity for those categories is itself less concentrated. Many more cybercriminals at varying levels of sophistication are participating in darknet market sales and scamming, so it makes sense we'd see those cybercriminals' funds dispersed across more deposit addresses for money laundering — each player may follow their own strategy. For more sophisticated forms of cybercrime like ransomware, administrators at the biggest ransomware strains account for a greater share of all activity, so we'd expect to see their money laundering be more concentrated as well.

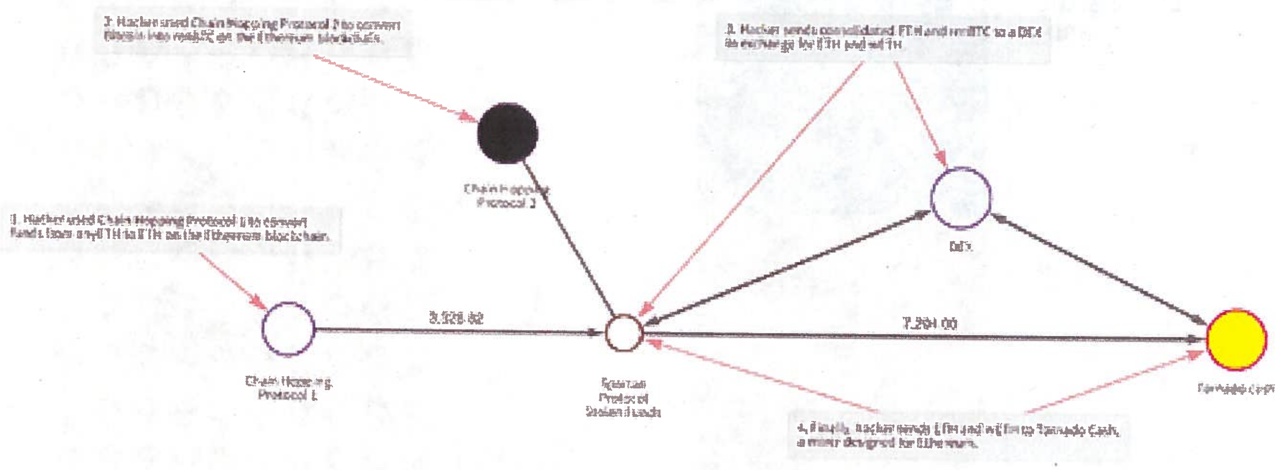
In 2021, money laundering activity in crypto was heavily concentrated.



Case study: Spartan Protocol hacker uses DeFi protocols and chain hopping to launder stolen funds

As we discussed above, usage of DeFi protocols for money laundering skyrocketed in 2021. The Spartan Protocol hack provides a good example of what this activity looks like.

In May 2021, one or more hackers exploited a code vulnerability to steal over $30 million worth of cryptocurrency from the protocol — mostly its native SPARTA token. The hacker then converted much of those funds into anyETH and anyBTC, which are Ethereum and Bitcoin composites respectively built on separate blockchains than the originals. Some of that anyBTC was then swapped for Bitcoin, thereby moving to the Bitcoin blockchain, which brings us to the transactions seen on the Chainalysis Reactor graph below.


2. Hacker used Chain Hopping Protocol 2 to convert Bitcoin into renBTC on the Ethereum blockchain.
3. Hacker sends consolidated ETH and renBTC to a DEX to exchange for ETH and wETH.
Chain Hopping Protocol 2
1. Hacker used Chain Hopping Protocol 1 to convert funds from anyETH to ETH on the Ethereum blockchain.
DEX
3,526.82
7,264.00
Chain Hopping Protocol 1
Spartan Protocol Stolen Funds
Tornado Cash
4. Finally, hacker sends ETH and wETH to Tornado Cash, a mixer designed for Ethereum.

Using two DeFi protocols that specialize in cross-chain transactions, the hacker chain hopped to the Ethereum blockchain, converting funds into Ethereum and renBTC. The hacker then sent those funds to a DEX, swapping them for new Ethereum and wrapped Ethereum. Finally, the hacker sent those funds to Tornado Cash, a mixer for the Ethereum blockchain.

While most of these transactions took place in the days immediately following the hack in early May, several took place months later, with the hacker continuing to launder funds well into October. This would be less likely to happen with centralized services, which unlike DeFi protocols typically ask customers for KYC information upon signup and have more ability as custodial platforms to freeze funds from suspicious sources. The Spartan Protocol hack is a great example not just of why DeFi holds appeal as a money laundering mechanism, but also of how complex investigations can become when cybercriminals use DeFi — especially chain hopping protocols.

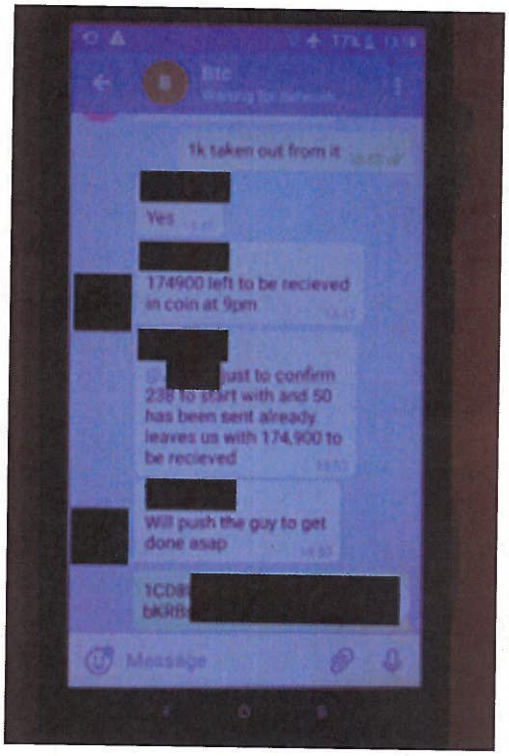
Law enforcement must become proficient in analyzing DeFi transactions in order to crack cases like that of the Spartan Protocol hack, but the teams behind DeFi protocols must also work to prevent their products from being abused by cybercriminals. One way they can do that is by screening the wallets interacting with their smart contracts for prior transactions with known illicit addresses. With the Chainalysis API, DeFi teams can automate the screening process and ensure that their protocols aren't being used to facilitate money laundering. If you work in DeFi, contact us here to learn more about automated wallet screening.

Case study: UK-based drug traffickers work with broker to launder drug money with Bitcoin

As we discussed previously, it's difficult to measure cryptocurrency's role in money laundering of funds derived from traditional, offline crimes. That's because in those cases, the cryptocurrency isn't moving from addresses that we've previously identified as associated with crime, but rather is initially deposited as fiat currency with no evidence of its criminal origins visible on the blockchain. The only way someone could know the origins of those funds would be if they were already investigating the criminals in question, and we know anecdotally that at least some criminals are doing this. Investigators can still use Chainalysis Reactor to investigate these cases, and we'll show you an example of how they do it in the following case study involving the successful investigation of a UK-based drug trafficking group.

The scheme was simple: The group supplied drugs across northern England and distributed them to street-level dealers, who would then sell them for cash which was later delivered back to the crime group. A courier would then collect the cash and deliver it to a broker who would arrange for the funds to be converted into bitcoin. The broker would then send the bitcoin to an address specified by the crime group, taking a small 4% fee. The Bitcoin network is essentially used as a value transfer system, and further analysis showed that the funds were ultimately sent to an OTC service nested at a popular cryptocurrency exchange.

Greater Manchester Police's Serious and Organised Crime Group discovered Bitcoin's role in the money laundering operation after pulling over one of the couriers, whom they'd previously observed collecting cash from a safe house, finding £170,000 in cash concealed in his vehicle. Police arrested the suspect for money laundering and seized two mobile phones. A subsequent digital forensic examination of these devices showed



Btc
Waiting for network...

1k taken out from it

[redacted]
Yes

[redacted]
[redacted]
174900 left to be recieved in coin at 9pm

[redacted]
[redacted] just to confirm
238 to rt with and 50 has been sent already leaves us with 174,900 to be recieved

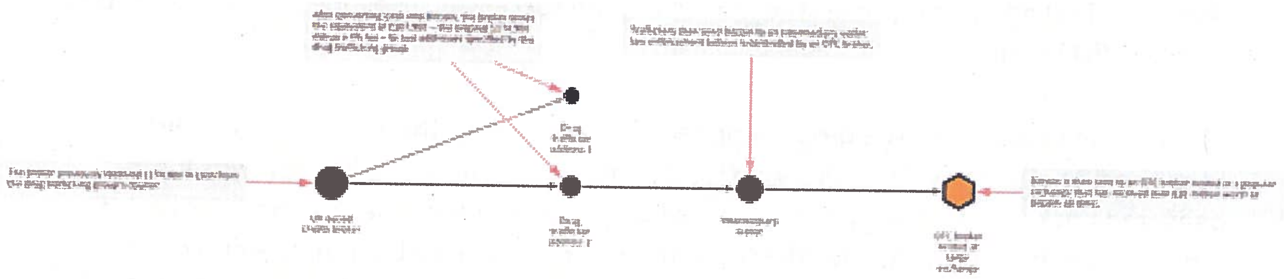
[redacted]
[redacted]
Will push the guy to get done asap

1CD8[redacted]
bKRB

various WhatsApp and Telegram messages detailing the plan, complete with Bitcoin addresses and screenshots of transaction hashes.

With this information, the officers were able to utilize blockchain analysis to see the flow of funds. Using Chainalysis Reactor, we can see the activity discussed in the message screenshot.

An equivalent of £174,900 minus a 4% brokers fee was sent in bitcoin to the address specified by the traffickers. This represents a relatively low fee in comparison to more traditional money laundering typologies, suggesting that Bitcoin-based laundering could become increasingly attractive to traditional criminals. The funds are then sent to an intermediary wallet before being deposited to an OTC service nested at a popular cryptocurrency exchange. Analysis of other transactions yielded evidence that the courier working for the drug trafficking group laundered at least £1 million across several Bitcoin transactions using these methods.



The case shows how important it is for all criminal investigators — not just those tasked with cybercrime cases — to understand cryptocurrency and blockchain analysis. It also serves as an example of how blockchain analysis can supplement more established investigative techniques law enforcement is already well-versed in. In this case, officers used digital forensic analysis to discover a cryptocurrency nexus, and from there were able to analyze transactions on the blockchain to gain an understanding of the drug traffickers' money laundering scheme, leading to successful prosecutions.

Criminal Balances

Criminal Whales Hold over $25 Billion in Cryptocurrency From Multitude of Illicit Sources

One positive development in the last year has been law enforcement's growing ability to seize cryptocurrency from criminals. We saw several examples of this in 2021, including:

- The U.S. Department of Justice (DOJ) seizing $2.3 million worth of cryptocurrency from the DarkSide ransomware operators responsible for the attack on Colonial Pipeline, as we cover in-depth in our ransomware section.
- IRS-CI's cumulative seizures of over $3.5 billion worth of cryptocurrency over the course of 2021.
- London's Metropolitan Police Service (MPS) made the UK's largest ever seizure of cryptocurrency, taking £180 million worth from a suspected money launderer.

More recently in February 2022, the DOJ seized $3.6 billion worth of Bitcoin connected to the 2016 hack of Bitfinex, in what is currently the largest ever recovery of stolen assets in either cryptocurrency or fiat.

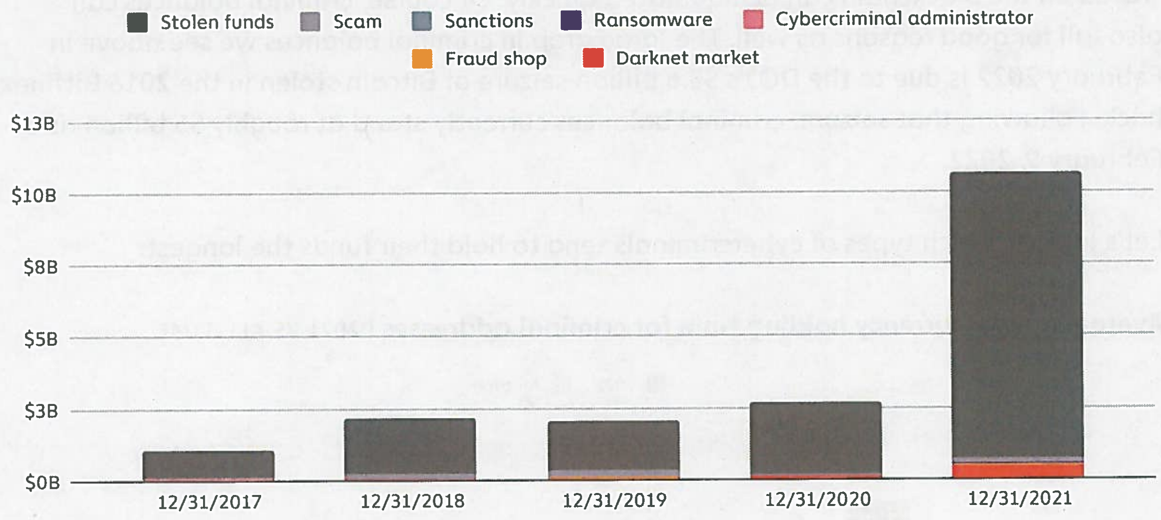
These stories are important not only because they allow financial restitution for victims of cryptocurrency-based crime, but also because they disprove the narrative that cryptocurrency is an untraceable, unseizable asset perfect for crime. If cybercriminals know law enforcement is capable of seizing their cryptocurrency, it may lower their incentive to use it in the future.

These cases also raise an important question: How much cryptocurrency is currently held by known criminal entities on the blockchain, and could therefore theoretically be seized by law enforcement? The answer is a function not just of cryptocurrency-based crime revenue in 2021, but of the all-time criminal revenue still held by visible addresses. Below, we'll break down both the sum amount of cryptocurrency holdings that can be traced back to illicit sources, as well as the total balances of criminal whales, meaning criminals holding $1 million or more in cryptocurrency.

Stolen funds dominate total criminal balances

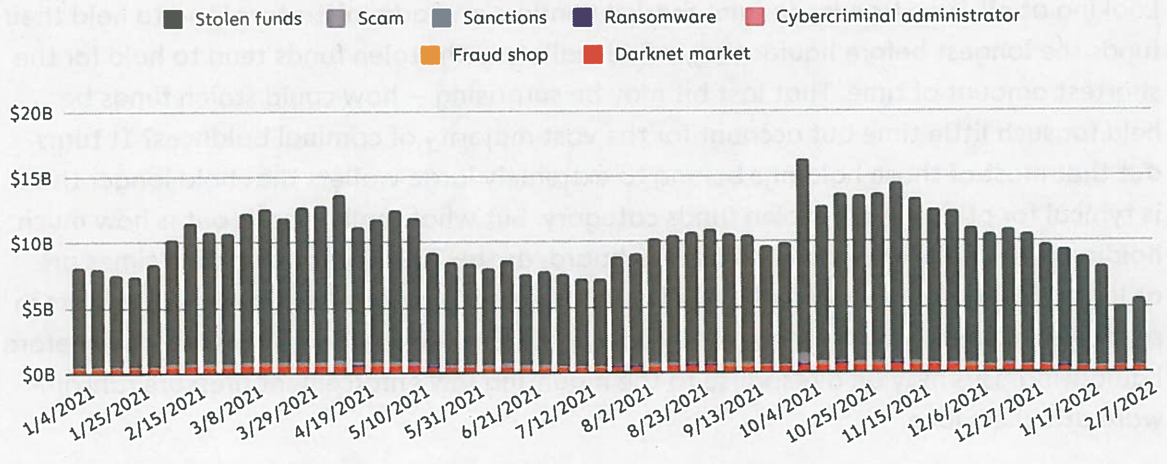
Let's start by looking at the year-end criminal balances over the last five years, broken down by the types of illicit activity the funds were derived from. In this analysis, criminal balances refer to any funds currently held by addresses Chainalysis has attributed to illicit actors. These addresses can belong to criminal services, like darknet markets, but in some cases can also be hosted by private wallets, such as in cases involving stolen funds.

Year end criminal balances | 2017–2021



Two things stand out most: The first is the huge increase in criminal balances in 2021 — at year's end, criminals held $11 billion worth of funds with known illicit sources, compared to just $3 billion at the end of 2020. The second is how much stolen funds dominate. As of the end of 2021, stolen funds account for 93% of all criminal balances at $9.8 billion. Darknet market funds are next at $448 million, followed by scams at $192 million, fraud shops at $66 million, and ransomware at $30 million.

Total weekly criminal balances by crime type | 2021

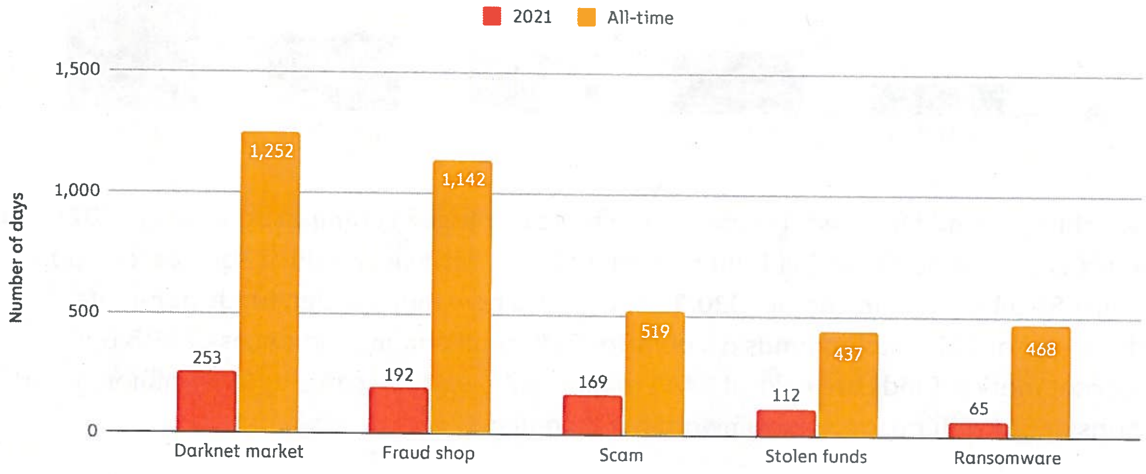


Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

Criminal balances also fluctuated throughout the year, from a low of $6.6 billion in July to a high of $14.8 billion in October. The fluctuations are a reminder of the importance of speed in cryptocurrency investigations, as criminal funds that have been successfully traced on the blockchain can be liquidated quickly. Of course, criminal balances can also fall for good reasons as well. The large drop in criminal balances we see above in February 2022 is due to the DOJ's $3.6 billion seizure of Bitcoin stolen in the 2016 Bitfinex hack. Following that seizure, criminal balances currently stand at roughly $5 billion as of February 9, 2022.

Let's look at which types of cybercriminals tend to hold their funds the longest.

Average cryptocurrency holding time for criminal addresses | 2021 VS ALL-TIME



Looking at all-time trends, darknet market vendors and administrators tend to hold their funds the longest before liquidating, while wallets with stolen funds tend to hold for the shortest amount of time. That last bit may be surprising — how could stolen funds be held for such little time but account for the vast majority of criminal balances? It turns out that most of those holdings belong to extremely large wallets that hold longer than is typical for others in the stolen funds category. But what really stands out is how much holding times have decreased across the board, as the 2021 average holding times are at least 75% shorter than the all-time figures in all categories. Ransomware operators in particular exemplify this trend, as they now hold funds on average for just 65 days before liquidating. This may be a response to the mounting law enforcement pressure ransomware attackers face.

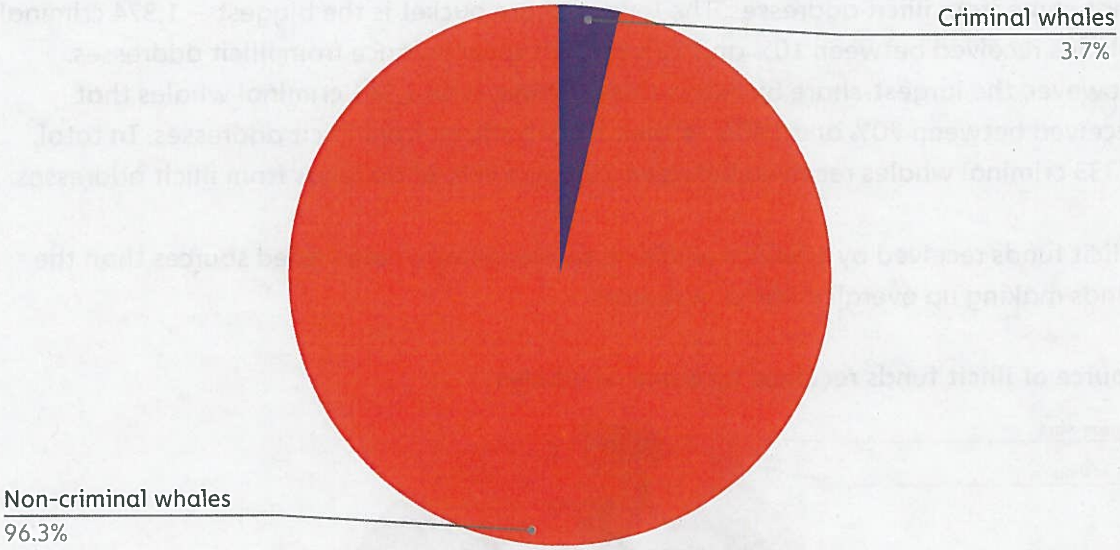
Criminal whales show more variation

A question that naturally follows from our investigation into criminal balances: Which criminals hold the most cryptocurrency? We decided to investigate by analyzing the balances of criminal whales. However, please note that we calculate criminal whale balances a bit differently than we do the overall criminal balances we discussed above. We define a criminal whale as any private wallet holding $1 million or more worth of cryptocurrency that has received more than 10% of its funds from illicit addresses.

Please recognize that because criminal whale balances are calculated based on private wallet holdings, while overall criminal balances are calculated based on the holdings of addresses tagged as illicit (meaning they can include funds held at services in addition to private wallets), the criminal whale balances discussed here won't align with the overall criminal balances calculated above.

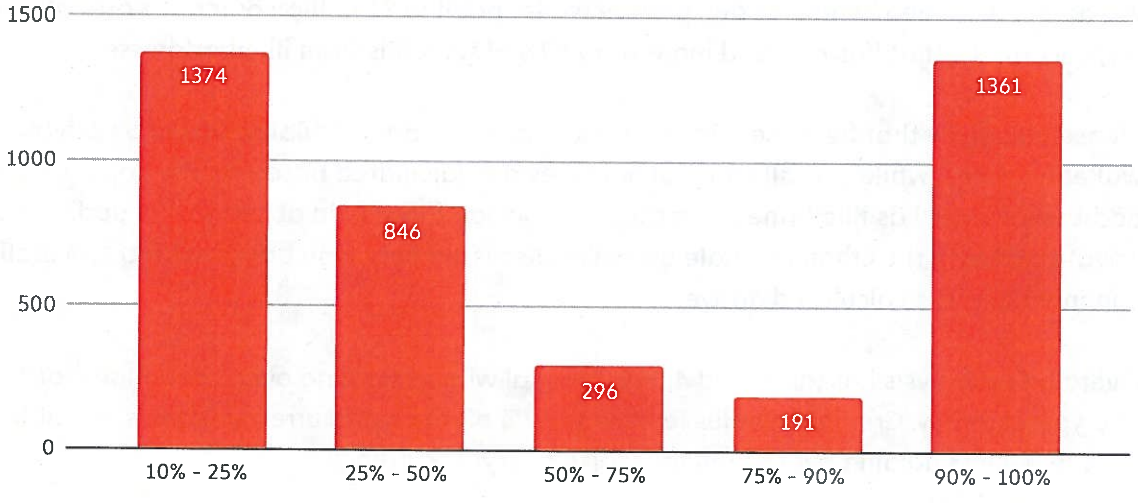
Overall, Chainalysis has identified 4,068 criminal whales holding over $25 billion worth of cryptocurrency. Criminal whales represent 3.7% of all cryptocurrency whales — that is, private wallets holding over $1 million worth of cryptocurrency.

Share of all cryptocurrency whales that received 10% or more of funds from illicit addresses



An interesting pattern emerges when we break down all criminal whales by the share of their total funds that have illicit origins: Most criminal whales received either a relatively small or extremely large share of their total balance from illicit addresses.

Criminal whales by share of all funds received from illicit addresses

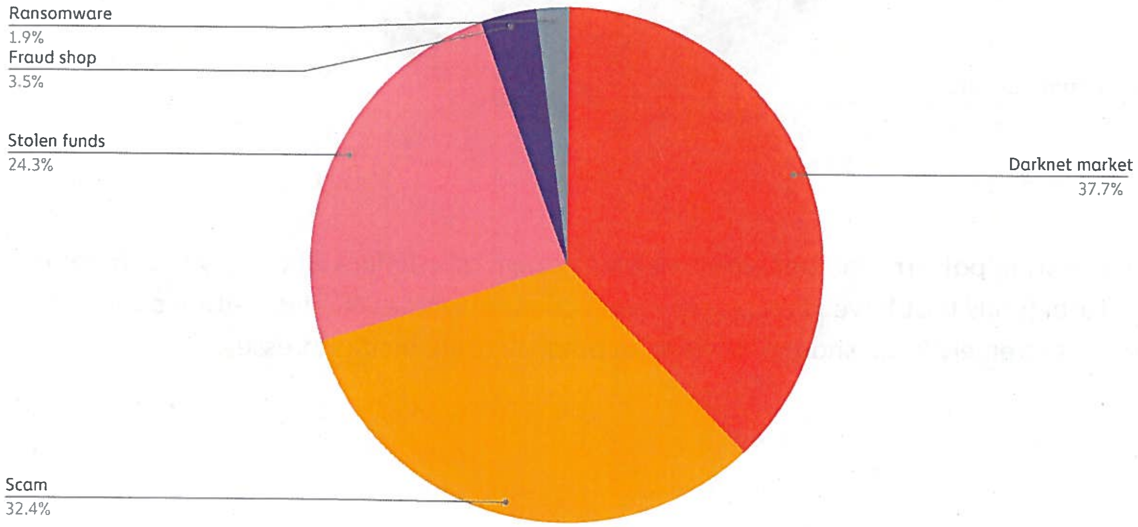


Share of all funds received from illicit addresses

Above, we bucket all criminal whales by the share of their total cryptocurrency received that came from illicit addresses. The lowest-share bucket is the biggest — 1,374 criminal whales received between 10% and 25% of their total balance from illicit addresses. However, the largest-share bucket is close behind, with 1,361 criminal whales that received between 90% and 100% of their total balance from illicit addresses. In total, 1,333 criminal whales received between 25% and 90% of all funds from illicit addresses.

Illicit funds received by criminal whales also come from more varied sources than the funds making up overall criminal balances.

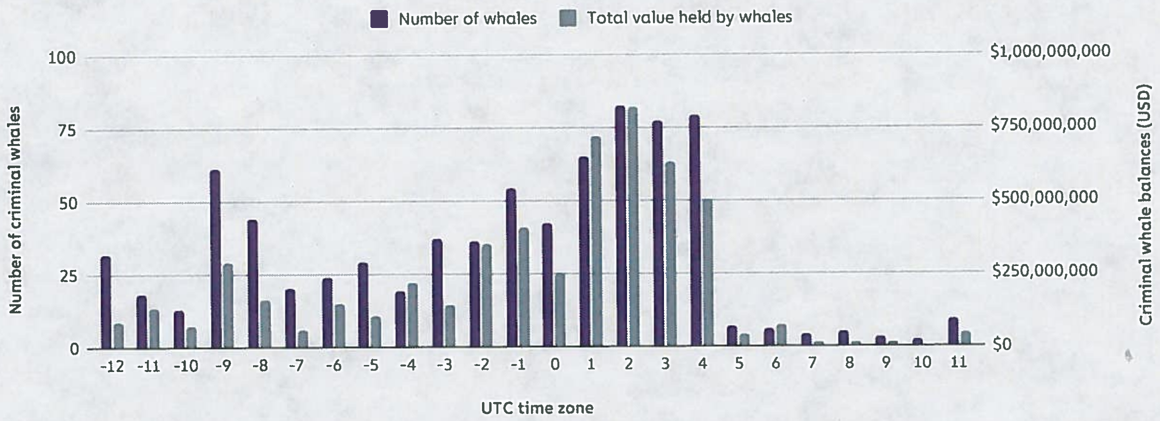
Source of illicit funds received by criminal whales



Whereas stolen funds dominate overall criminal balances, darknet markets are the biggest source of illicit funds sent to criminal whales, followed by scams second and stolen funds third.

Finally, we can also use time zone analysis to try and approximate the location of criminal whales. On the graph below, we've assigned UTC time zones to the 768 criminal whales whose wallets have enough activity for us to make a strong estimate.

Estimated UTC time zone of criminal whales



UTC time zones 2, 3, and 4 are estimated to contain the most criminal whales, while time zones 1 and -9 also have a large number. UTC time zones 2, 3, and 4 include much of Russia, including major population centers like Moscow and Saint Petersburg, which is especially interesting in the context of Russia's outsized role in cryptocurrency-based crime, as we explore elsewhere in this report. However, time zones of course only allow us to estimate longitudinal location, so it's possible some of these criminal whales are based in other countries within time zones 2, 3, and 4, such as South Africa, Saudi Arabia, or Iran.

The ability to efficiently track criminal whales and quantify their holdings from one public data set is a major difference between cryptocurrency-based crime and fiat-based crime. In fiat, the highest net worth criminals have murky networks of foreign banks and shell corporations to obfuscate their holdings. But in cryptocurrency, transactions are saved on the blockchain for all to see. Investigation of criminal whales represents a significant opportunity for government agencies around the world to continue their string of successful seizures, and bring to justice the biggest beneficiaries of cryptocurrency-based crime.

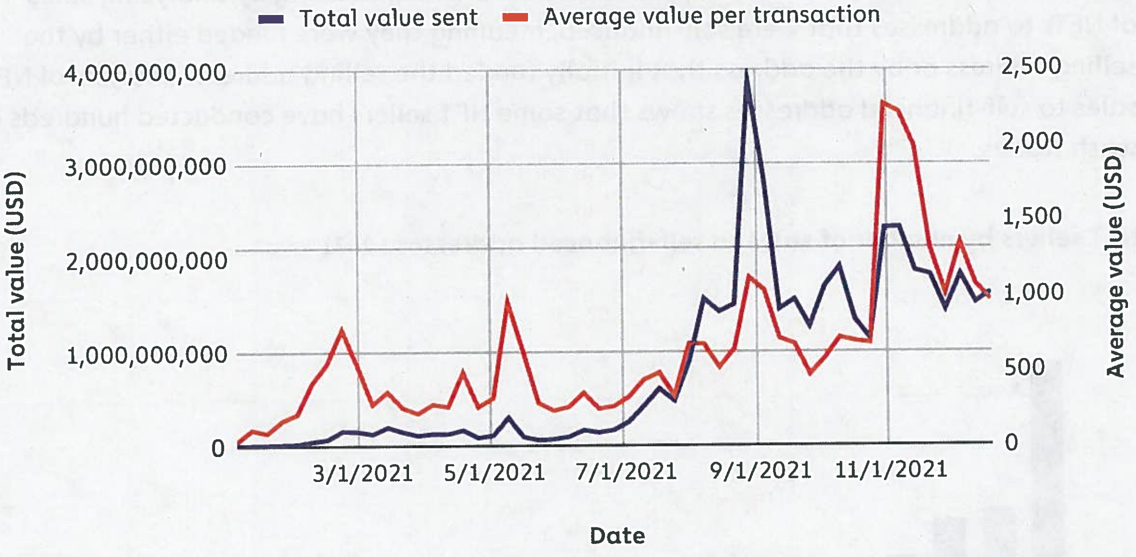
NFTs and Crime

Chainalysis Detects Significant Wash Trading and Some Money Laundering In this Emerging Asset Class

Non-fungible tokens (NFTs) were one of the biggest stories in cryptocurrency in 2021. NFTs are blockchain-based digital items whose units are designed to be unique, unlike traditional cryptocurrencies whose units are meant to be interchangeable. NFTs can store data on blockchains — with most NFT projects built on blockchains like Ethereum and Solana — and that data can be associated with images, videos, audio, physical objects, memberships, and countless other developing use cases. NFTs typically give the holder ownership over the data or media the token is associated with, and are commonly bought and sold on specialized marketplaces.

NFT popularity skyrocketed in 2021. Chainalysis tracked a minimum $44.2 billion worth of cryptocurrency sent to ERC-721 and ERC-1155 contracts — the two types of Ethereum smart contracts associated with NFT marketplaces and collections — up from just $106 million in 2020.

Weekly total cryptocurrency value and average value per transaction sent to NFT platforms | 2021



However, as is the case with any new technology, NFTs offer potential for abuse. It's important that as our industry considers all the ways this new asset class can change how we link the blockchain to the physical world, we also build products that make NFT investment as safe and secure as possible. Below, we look at two forms of illicit activity we've observed in NFTs:

- Wash trading to artificially increase the value of NFTs
- Money laundering through the purchase of NFTs

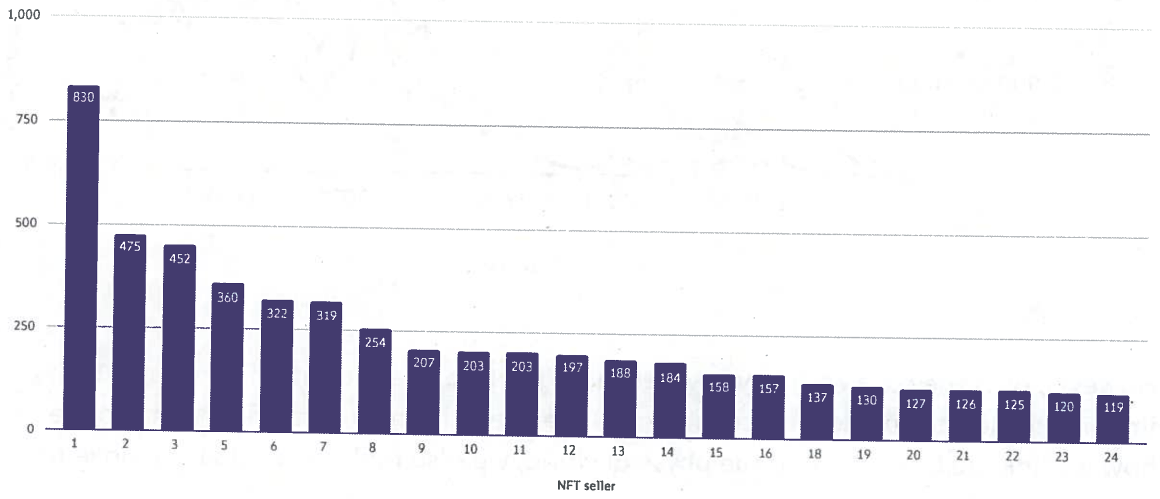
Let's dive in.

Some NFT sellers are making a killing with wash trading

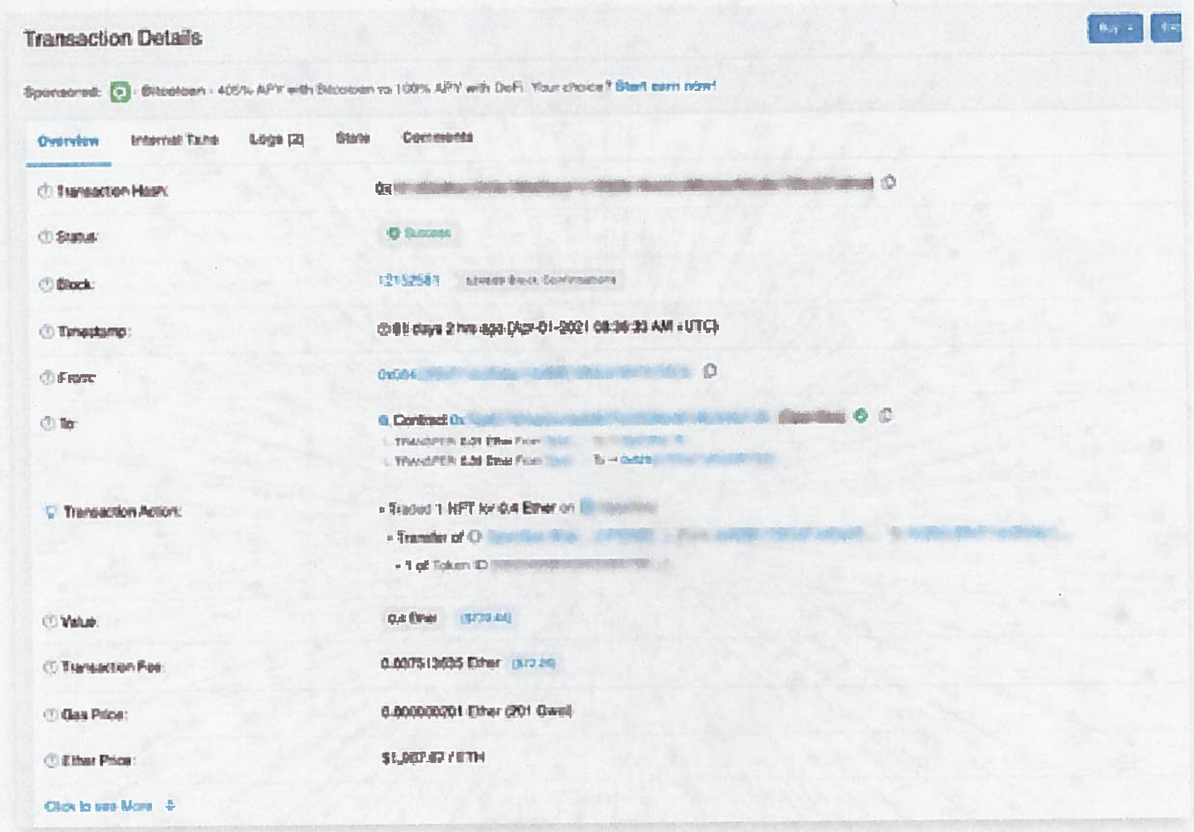
Wash trading, meaning executing a transaction in which the seller is on both sides of the trade in order to paint a misleading picture of an asset's value and liquidity, is another area of concern for NFTs. Wash trading has historically been a concern with cryptocurrency exchanges attempting to make their trading volumes appear greater than they are. In the case of NFT wash trading, the goal would be to make one's NFT appear more valuable than it really is by "selling it" to a new wallet the original owner also controls. In theory, this would be relatively easy with NFTs, as many NFT trading platforms allow users to trade by simply connecting their wallet to the platform, with no need to identify themselves.

With blockchain analysis, however, we can track NFT wash trading by analyzing sales of NFTs to addresses that were self-financed, meaning they were funded either by the selling address or by the address that initially funded the selling address. Analysis of NFT sales to self-financed addresses shows that some NFT sellers have conducted hundreds of wash trades.

NFT sellers by number of sales to self-financed addresses | 2021



Let's look more closely at Seller 1, the most prolific NFT wash trader on the chart above, who has made 830 sales to addresses they've self-financed. The Etherscan screenshot below shows a transaction in which that seller, using the address beginning 0x828, sold an NFT to the address beginning 0x084 for 0.4 Ethereum via an NFT marketplace.



Transaction Details

Sponsored: Bitcoinan · 405% APY with Bitcoinan vs 100% APY with DeFi. Your choice? Start earn now!

Overview | Internal Txns | Logs (2) | State | Comments

Transaction Hash: 0x[redacted]

Status: Success

Block: 12152581 [illegible] Block Confirmations

Timestamp: 81 days 2 hrs ago (Apr-01-2021 08:36:33 AM +UTC)

From: 0x084[redacted]

To: Contract 0x[redacted]
- TRANSFER 0.01 Ether From [redacted] To [redacted]
- TRANSFER 0.39 Ether From [redacted] To → [redacted]

Transaction Action:
- Traded 1 NFT for 0.4 Ether on [redacted]
- Transfer of [redacted]
- 1 of Token ID [redacted]

Value: 0.4 Ether ($770.44)

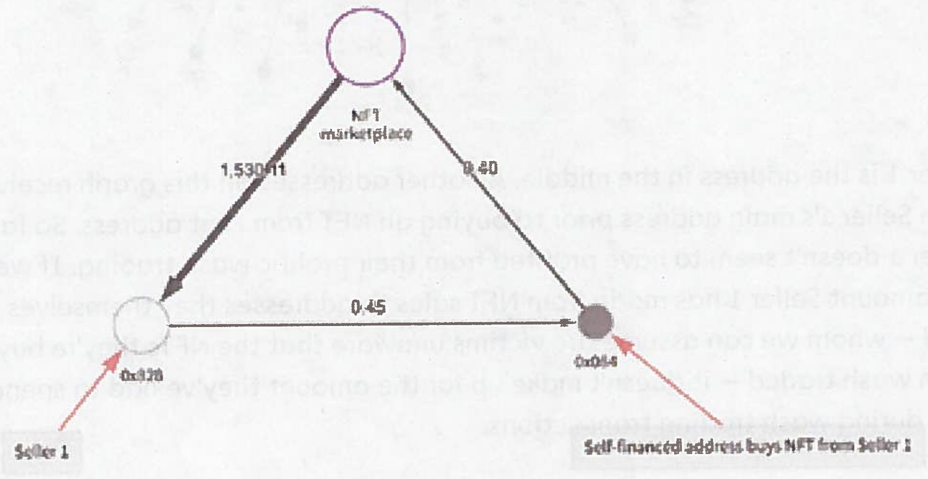
Transaction Fee: 0.00751365 Ether ($12.28)

Gas Price: 0.000000201 Ether (201 Gwei)

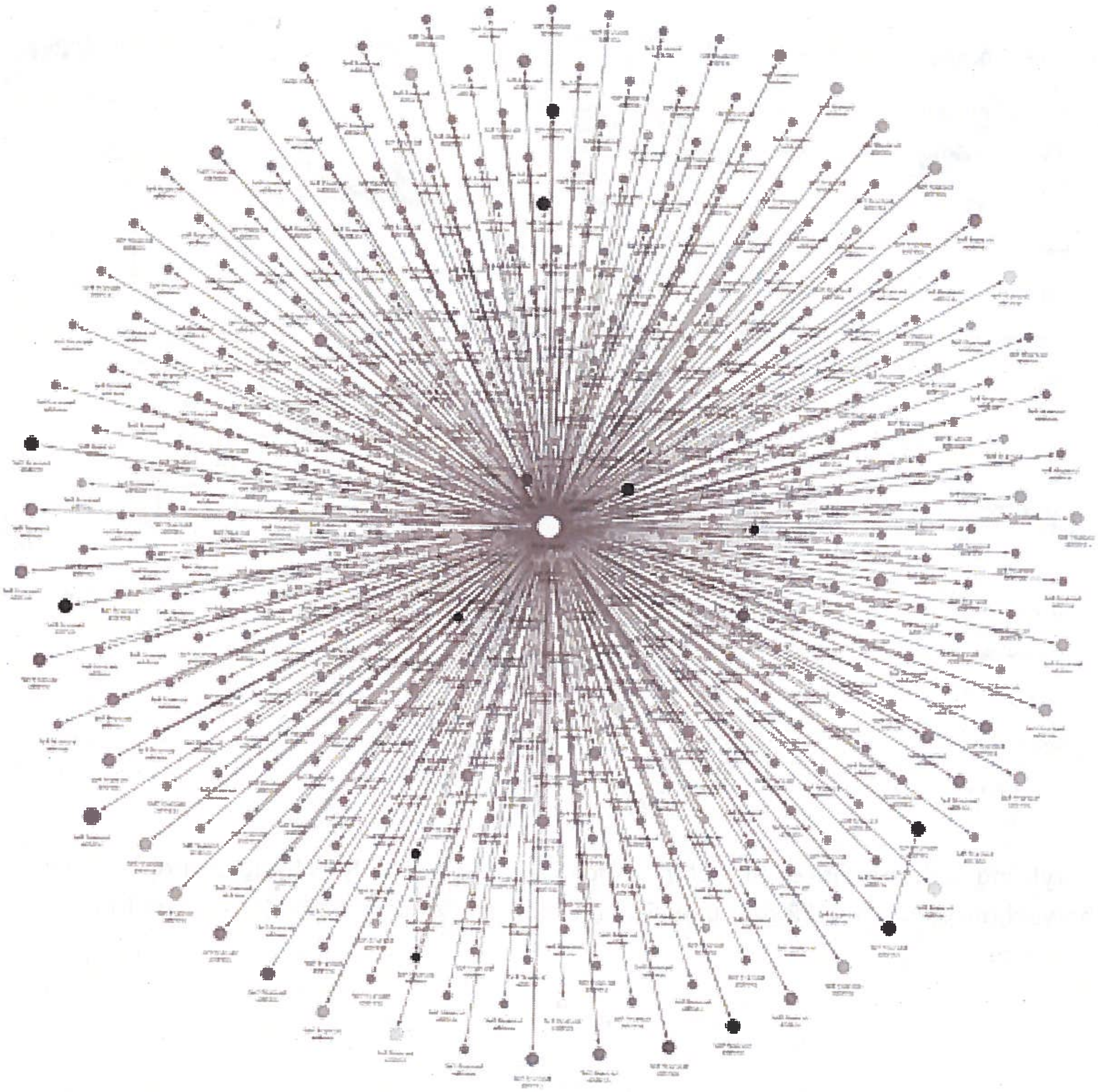
Ether Price: $1,907.87 / ETH

Click to see More

Everything looks normal at first glance. However, the Chainalysis Reactor graph below shows that address 0x828 sent 0.45 Ethereum to that address 0x084 shortly before that sale.



This activity fits a pattern for Seller 1. The Reactor graph below shows similar relationships between Seller 1 and hundreds of other addresses to which they've sold NFTs.



Seller 1 is the address in the middle. All other addresses on this graph received funds from Seller 1's main address prior to buying an NFT from that address. So far though, Seller 1 doesn't seem to have profited from their prolific wash trading. If we calculate the amount Seller 1 has made from NFT sales to addresses they themselves did not fund — whom we can assume are victims unaware that the NFTs they're buying have been wash traded — it doesn't make up for the amount they've had to spend on gas fees during wash trading transactions.

Seller 1 address	Amount spent on gas fees in wash trading transactions	Revenue from sales of wash traded NFTs to victims	Profits
0x828...	- $35,642	$27,258	- $8,383

However, the story changes if we look at a bigger piece of the NFT ecosystem. Using blockchain analysis, we identified 262 users who have sold an NFT to a self-financed address more than 25 times. While we can't be 100% sure that all instances of NFT sales to self-financed wallets are intended for wash trading, the 25-transaction threshold gives us a higher degree of confidence that these users are habitual wash traders. Just as we did above for one wash trader, we calculated these 262 wash traders' overall profits by subtracting the amount they've spent on gas fees from the amount they've made selling NFTs to unsuspecting buyers. One caveat for this analysis is that it only captures trades made in Ethereum and Wrapped Ethereum, so there's likely wash trading activity we're not considering here.

Nonetheless, an interesting story emerges: Most NFT wash traders have been unprofitable, but the successful NFT wash traders have profited so much that, as a whole, this group of 262 has profited immensely overall.

Wash trader group	Number of addresses	Profits from wash trading
Profitable wash traders	110	$8,875,315
Unprofitable wash traders	152	- $416,984
All	262	$8,458,331

The 110 profitable wash traders have collectively made nearly $8.9 million in profit from this activity, dwarfing the $416,984 in losses made by the 152 unprofitable wash traders. Even worse, that $8.9 million is most likely derived from sales to unsuspecting buyers who believe the NFT they're purchasing has been growing in value, sold from one distinct collector to another.

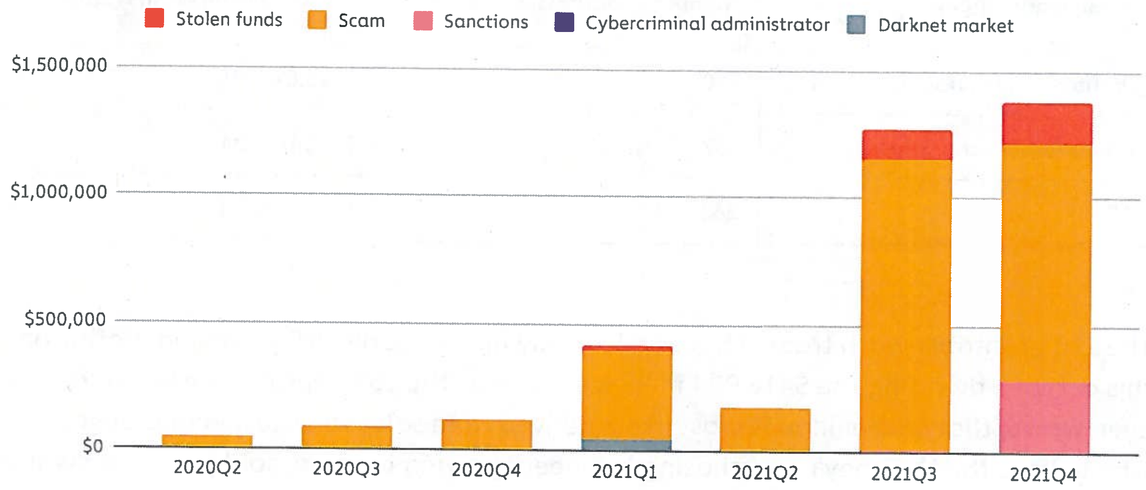
NFT wash trading exists in a murky legal area. While wash trading is prohibited in conventional securities and futures, wash trading involving NFTs has yet to be the subject of an enforcement action. However, that could change as regulators shift focus and apply existing anti-fraud authorities to new NFT markets. More generally, wash trading in NFTs can create an unfair marketplace for those who purchase artificially inflated tokens, and its existence can undermine trust in the NFT ecosystem, inhibiting future growth. We encourage NFT marketplaces to discourage this activity as much as possible. Blockchain data and analysis makes it easy to spot users who sell NFTs to addresses they've self-financed, so marketplaces may want to consider bans or other penalties for the worst offenders.

Money laundering activity small but visible in NFTs

Money laundering has long been an issue in the fine art world, and it's not hard to see why. As one 2019 article from the National Law Review points out, art pieces like paintings are easy to move, have relatively subjective prices, and may offer certain tax advantages. Criminals can therefore purchase art with illegally gained funds, sell them later, and poof — they have seemingly clean money with no connection to the original criminal activity. This background, along with the pseudonymity of cryptocurrency, has many wondering if NFTs are vulnerable to similar abuses. But while money laundering in physical art is difficult to quantify, we can make more reliable estimates of NFT-based money laundering thanks to the inherent transparency of the blockchain.

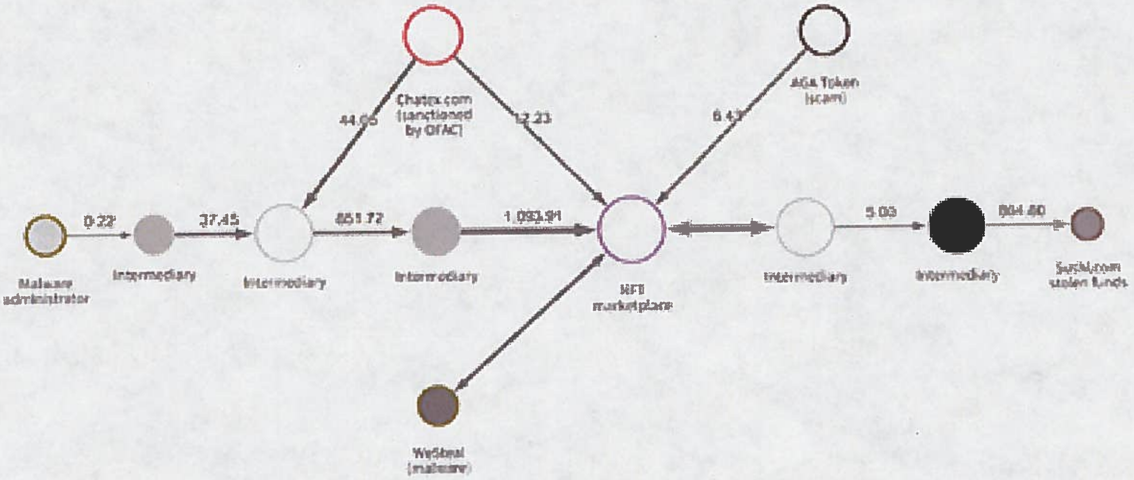
So, are cybercriminals using illicit funds to purchase NFTs? Let's take a look.

Illicit value received by NFT platforms | 2020Q2–2021Q4



Value sent to NFT marketplaces by illicit addresses jumped significantly in the third quarter of 2021, crossing $1 million worth of cryptocurrency. The figure grew again in the fourth quarter, topping out at just under $1.4 million. In both quarters, the vast majority of this activity came from scam-associated addresses sending funds to NFT marketplaces to make purchases. Both quarters also saw significant amounts of stolen funds sent to marketplaces as well. Perhaps most concerningly, in the fourth quarter, we saw roughly $284,000 worth of cryptocurrency sent to NFT marketplaces from addresses with sanctions risk. All of that was due to transfers from the P2P exchange Chatex, which the U.S. Treasury's Office of Foreign Asset Control (OFAC) added to its Specially Designated Nationals (SDN) list last year.

We can see examples of different types of criminals buying NFTs in the Reactor graph below.



Here, we can see addresses associated with several different types of cybercriminals sending funds to a popular NFT marketplace, including malware operators, scammers, and Chatex.

All of this activity represents a drop in the bucket compared to the $8.6 billion worth of cryptocurrency-based money laundering we tracked in all of 2021. Nevertheless, money laundering, and in particular transfers from sanctioned cryptocurrency businesses, represents a large risk to building trust in NFTs, and should be monitored more closely by marketplaces, regulators, and law enforcement.

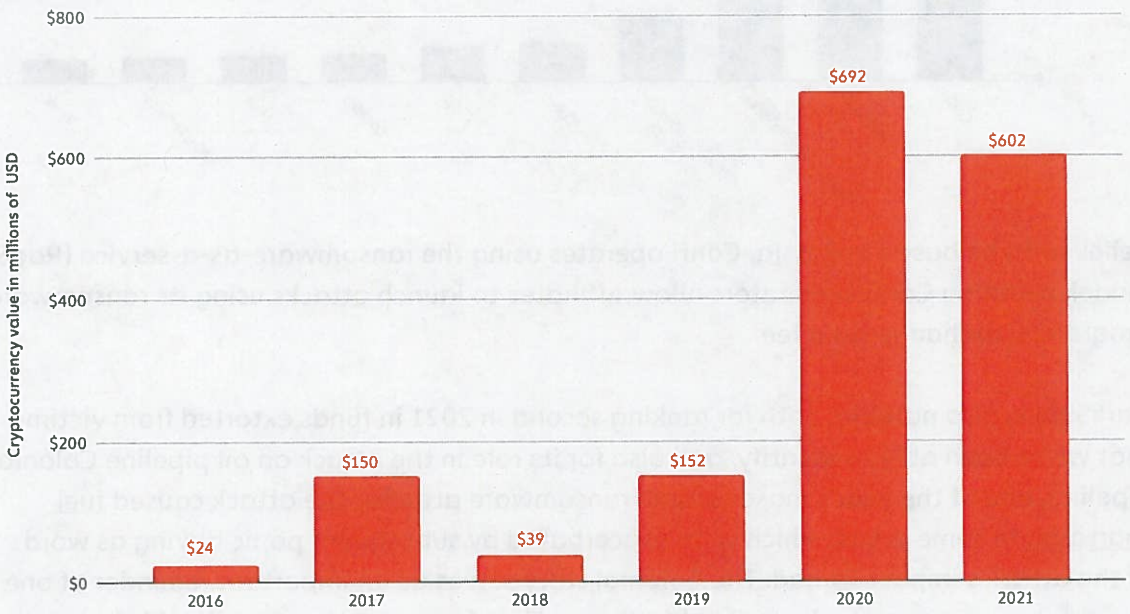
Ransomware

As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict

In our last Crypto Crime Report, we deemed 2020 the "Year of Ransomware" due to the huge growth in cryptocurrency extorted in ransomware attacks. When we first released that report last year, we announced that we had tracked roughly $350 million worth of payments from victims to ransomware operators. However, we explained at the time that this figure was likely an underestimate we would raise in the future due to both underreporting by ransomware victims and our continuing identification of ransomware addresses that have received previous victim payments.

Sure enough, we updated our ransomware numbers a few times throughout 2021, reflecting new payments we hadn't identified previously. As of January 2022, we've now identified just over $692 million in 2020 ransomware payments — nearly double the amount we initially identified at the time of writing last year's report.

Total cryptocurrency value received by ransomware addresses | 2016–2021

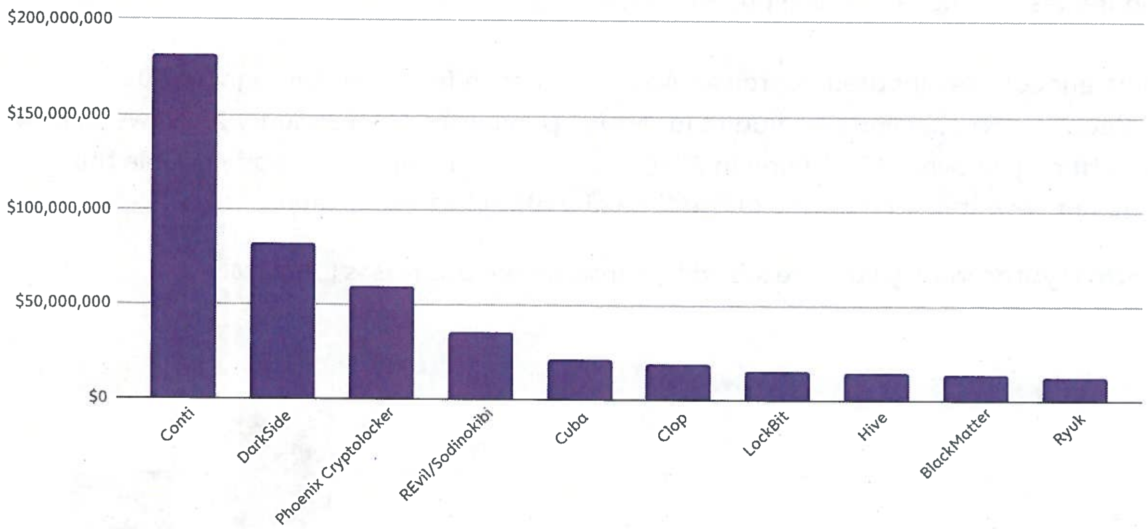


You'll also see above that as of now, we've identified just over $602 million worth of ransomware payments in 2021. However, just like last year, we know that this too is an underestimate, and that the true total for 2021 is likely to be much higher. In fact, despite these numbers, anecdotal evidence, plus the fact that ransomware revenue in the first half of 2021 exceeded that of the first half of 2020, suggests to us that 2021 will eventually be revealed to have been an even bigger year for ransomware. Below, we'll look more at which ransomware strains were most prolific in 2021, how ransomware operators laundered their funds, and examples of how law enforcement and security agencies are fighting back against ransomware.

2021 ransomware activity summarized

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $180 million from victims.

Top 10 ransomware strains by revenue | 2021

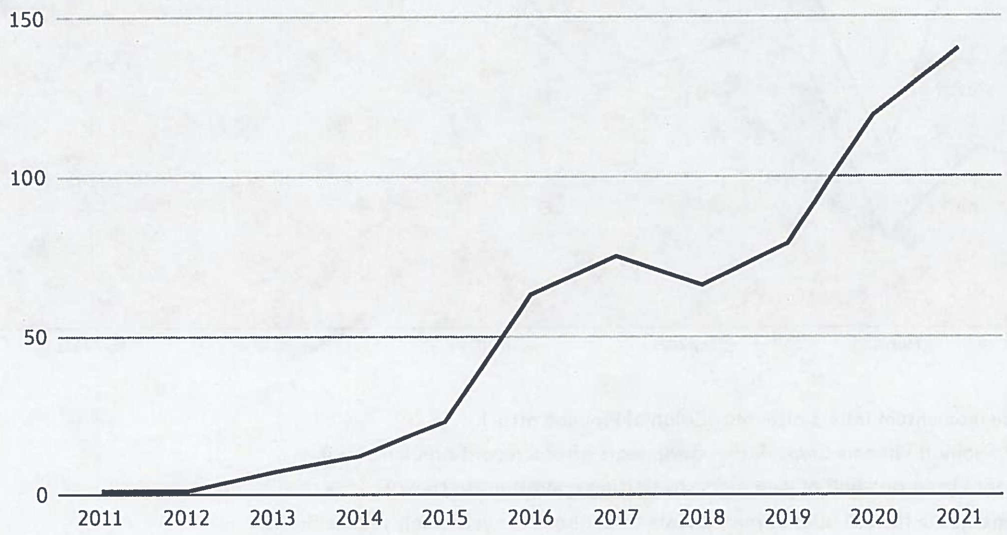


Believed to be based in Russia, Conti operates using the ransomware-as-a-service (RaaS) model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee.

DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were exacerbated by subsequent panic buying as word of the attack's impact spread. The Colonial story serves as an important reminder of one reason ransomware attacks are so dangerous: They frequently target critical infrastructure we need to keep the country running — not just energy providers, but food providers, schools, hospitals and financial services companies as well.

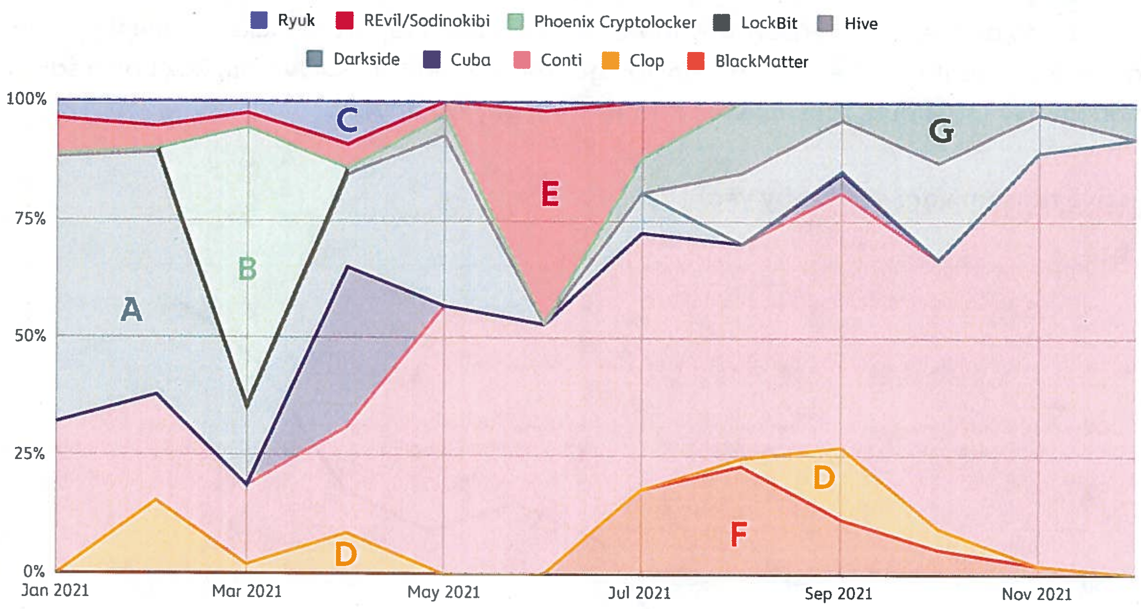
However, the Colonial Pipeline attack also turned into a success story, as the U.S. Department of Justice was able to track and seize $2.3 million of the ransom that Colonial paid to DarkSide. We'll look more at how agents were able to do this later in the section, but suffice it to say that law enforcement's growing ability to seize payments after they're made represents a huge step forward in the fight against ransomware. It also serves as one more reason why more victims should report attacks — even if you pay, law enforcement may be able to help you get those funds back. Overall, 2021 also saw more active individual ransomware strains than any other year.

Active ransomware strains by year | 2011–2021



At least 140 ransomware strains received payments from victims at any point in 2021, compared to 119 in 2020, and 79 in 2019. Those numbers are emblematic of the intense growth of ransomware we've seen over the last two years. Most ransomware strains come and go in waves, staying active for a short amount of time before becoming dormant. We show this on the graph below, which shows how the top ten ransomware strains ebbed and flowed in activity throughout the year.

Top 10 most active strains in 2021 by monthly revenue | JAN–NOV 2021



A DarkSide momentum falters after May Colonial Pipeline attack

B Evil Corp-spinoff Phoenix Cryptolocker disappears after a record-breaking haul

C Ryuk wanes in second half of year, perhaps shifting operations to Diavol

D Clop remerges in the fall after several arrests throughout the year likely reduce activity

E REvil sparked retirement rumors after Kaseya attack in July. It ultimately self-closed in Q4 under LE pressure

F BlackMatter picks up where DarkSide left off, but a decryptor released by Emsisoft likely depressed revenue

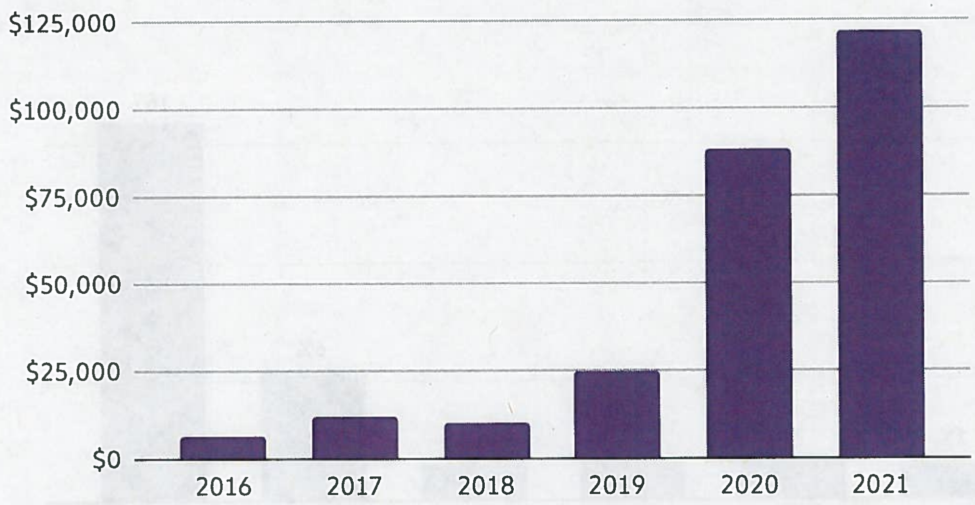
G LockBit went dark while it rebranded to LockBit 2.0 in June and remains a persistent threat into 2022

Conti was the one strain that remained consistently active for all of 2021, and in fact saw its share of all ransomware revenue grow throughout the year. Overall though, Conti's staying power is increasingly outside the norm.

As we'll explore more later on, the growing number of active strains and generally short lifespan of most strains is also a result of rebranding efforts. More and more in 2021, we've seen the operators of strains publicly "shut down" before re-launching under a new name, presenting themselves as a separate cybercriminal group. Often, the rebranded strain's financial footprint on the blockchain aligns with that of the original, which can tip investigators off as to who's really behind the new strain.

Ransomware payment sizes also continued to grow in 2021, a trend we've observed every year since 2018.

Average ransomware payment size | 2016–2021

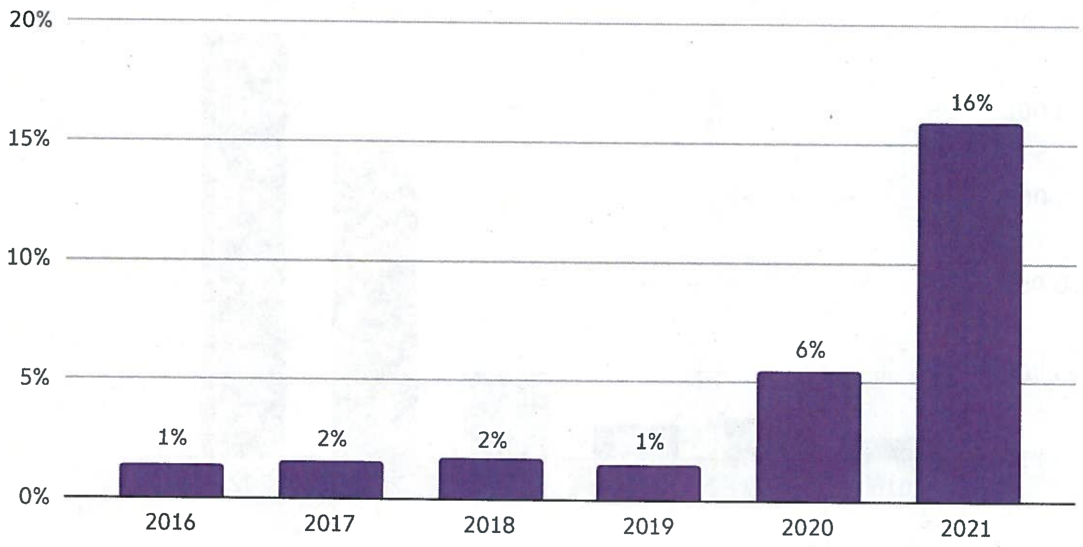


The average ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. Large payments such as the record $40 million received by Phoenix Cryptolocker spurred this all-time high in average payment size. One reason for the increase in ransom sizes is ransomware attackers' focus on carrying out highly-targeted attacks against large organizations. This "big game hunting" strategy is enabled in part by ransomware attackers' usage of tools provided by third-party providers to make their attacks more effective. These tools range from illicit hacking aids to legitimate products, and include:

- Rented infrastructure such as bulletproof web hosting, domain registration services, botnets, proxy services, and email services to carry out attacks.
- Hacking tools like network access to already-infiltrated networks, exploit kits that scan victims' networks for vulnerabilities, and malware programs that help attackers distribute ransomware more effectively.
- Stolen data such as passwords, individuals' personally identifiable information, and compromised remote desktop protocol (RDP) credentials, which help attackers break into victims' computer networks.

Usage of these services by ransomware operators spiked to its highest ever levels in 2021.

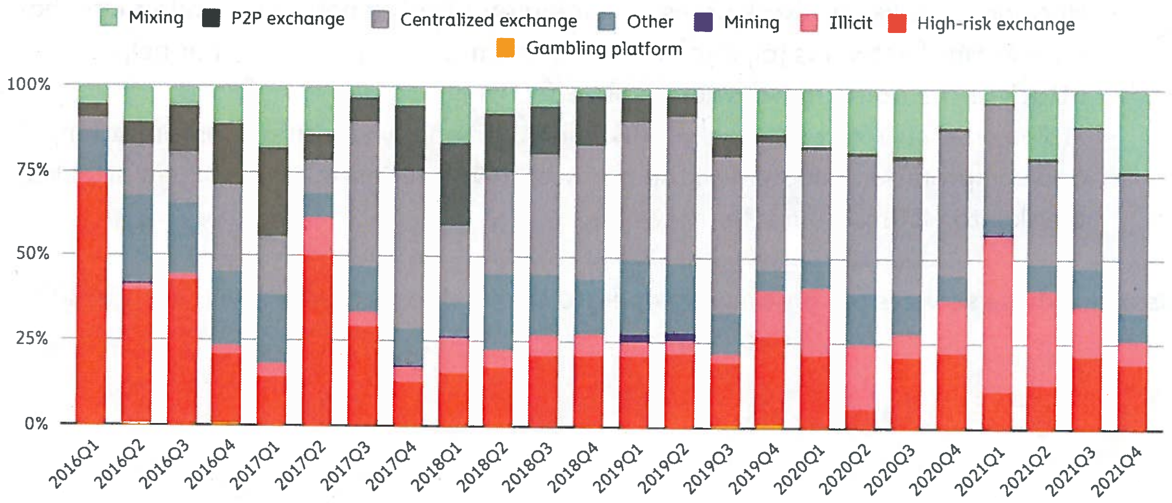
Share of ransomware funds going to third-party sellers | 2016–2021



16% of all funds sent by ransomware operators were spent on tools and services used to enable more effective attacks, compared to 6% in 2020. While it's possible some of that activity constitutes money laundering rather than the purchase of illicit services, we believe that increasing use of those services is one reason ransomware attackers became more effective in 2021, as evidenced by rising average victim payment sizes.

Another important trend to monitor in ransomware is money laundering. The graph below shows where attackers move the cryptocurrency they extort from victims.

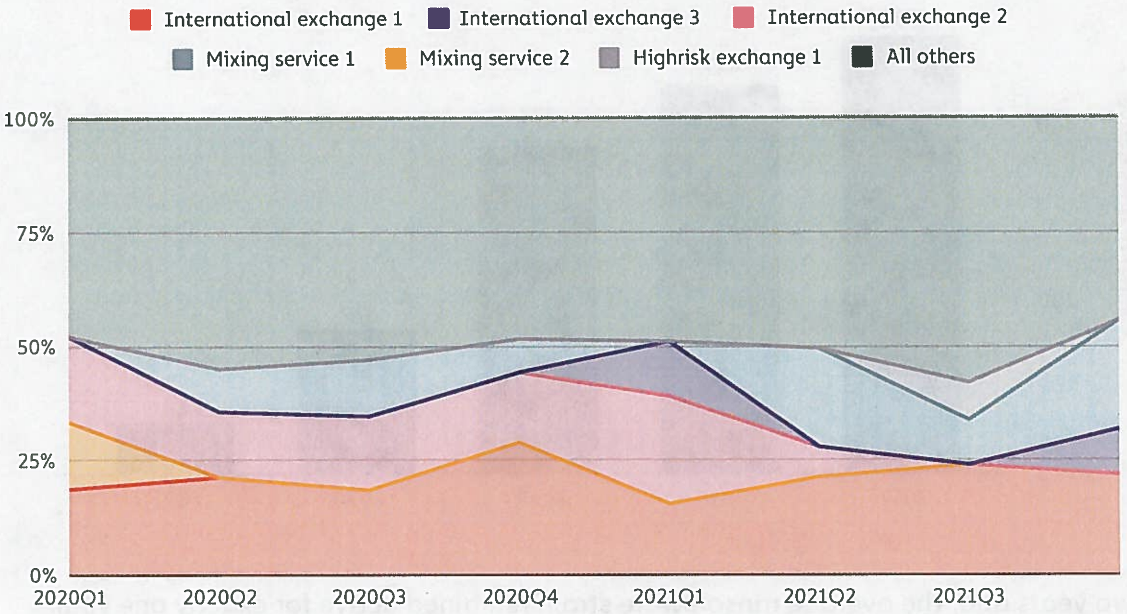
Destination of funds leaving ransomware addresses | 2016–2021



Over the last few years, most ransomware strains have laundered their stolen funds by sending them to centralized exchanges. Some are in the high-risk category, meaning that they tend to have relaxed compliance procedures, but mostly to mainstream exchanges with more established compliance programs. We also see substantial funds sent to both mixers and addresses associated with other forms of illicit activity.

The money laundering trends get even more interesting if we drill down to the individual services receiving funds from ransomware.

Services receiving funds from ransomware addresses | 2020–2021



Amazingly, 56% of funds sent from ransomware addresses since 2020 have wound up at one of six cryptocurrency businesses:

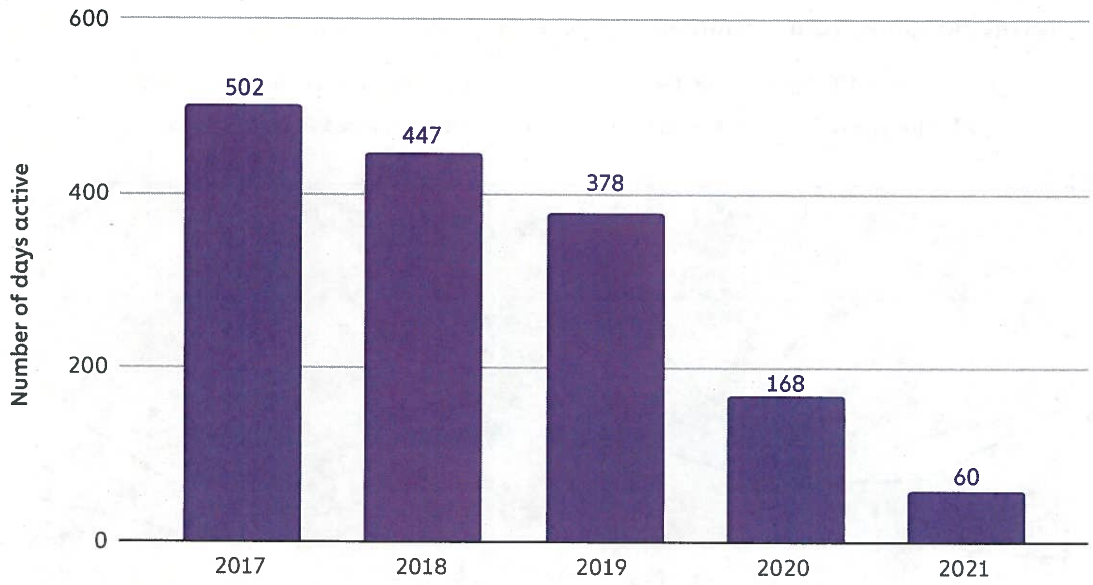
- Three large, international exchanges
- One high-risk exchange based in Russia
- Two mixing services

Similar to the rebranding activity we described above, these money laundering trends show how small the ransomware ecosystem really is. That's good news, as it means the strategy for fighting ransomware is likely simpler than it appears at first glance. By cracking down on the small number of services that facilitate this money laundering activity, law enforcement can significantly reduce attackers' options for cashing out, reducing the financial incentive to carry out ransomware attacks and hampering ransomware organizations' ability to operate.

2021's rebranding craze shows the ransomware ecosystem is smaller than we think

As we discussed above, most ransomware strains aren't active for very long. While this has always been the case to some degree, the trend has become even more pronounced in 2021.

Average lifespan of a ransomware strain | 2017–2021



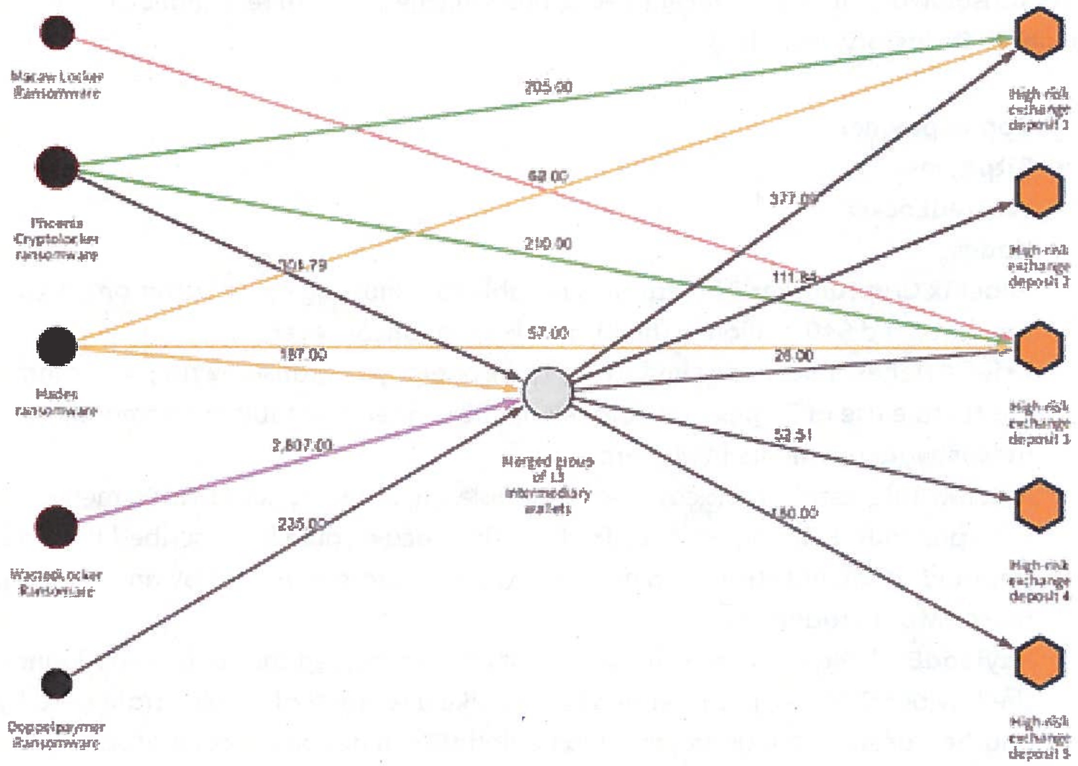
Two years ago, the average ransomware strain remained active for exactly one year. In 2021, the average strain is active for no more than two months. Why is the average ransomware lifespan dropping so quickly?

One big reason is rebranding. More than ever in 2021, cybersecurity researchers have noted instances of ransomware attackers publicly claiming to cease operations, only to relaunch later under a new name — the giveaway is usually similarities in the ransomware's code, as well as intelligence gathered from cybercriminal forums and blockchain analysis. So, while at least 140 ransomware strains were active in 2021, many of those strains were in fact run by the same cybercriminal groups.

These strains attempt to create the illusion that they belong to different cybercriminal organizations by setting up separate victim payment sites and other infrastructure, but share similarities in their code. Evil Corp, a Russia-based cybercriminal gang behind several ransomware attacks in recent years, has launched several rebranded strains throughout its history, including:

- **Doppelpaymer**
- **Bitpaymer**
- **WastedLocker**
- **Hades**
- **Phoenix Cryptolocker.** This strain is notable for "shutting down" after one attack that extorted $40 million — the largest known ransom ever paid.
- **Grief.** Grief exhibits code similarities to Doppelpaymer ransomware, including the telltale use of Dridex malware. As of 2021, Grief is notable for demanding ransomware payments in Monero.
- **Macaw.** Interestingly, Macaw uses a completely different negotiation method than previous Evil Corp strains. In this way, Macaw could be described less as a "rebrand" of an old strain and more as a unique strain launched by an existing ransomware organization.
- **PayloadBIN.** Many cybersecurity analysts have reported that Evil Corp's launch of the PayloadBIN strain is intended to look like a rebrand of an old strain used by another ransomware group, making PayloadBIN a double rebrand of sorts.

We can also see evidence of some of these strains' common ownership in their cryptocurrency transaction histories. Check out the Chainalysis Reactor graph below.

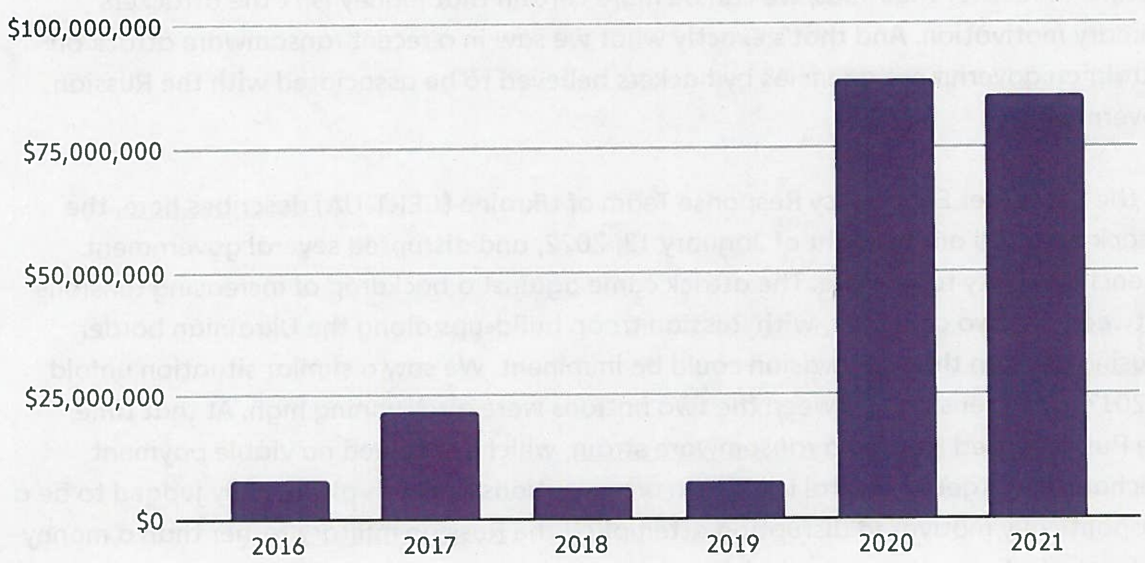

Macaw Locker Ransomware
Phoenix Cryptolocker ransomware
Hades ransomware
WastedLocker Ransomware
Doppelpaymer Ransomware
Merged group of 13 intermediary wallets
High-risk exchange deposit 1
High-risk exchange deposit 2
High-risk exchange deposit 3
High-risk exchange deposit 4
High-risk exchange deposit 5
705.00
69.00
210.00
301.79
57.00
187.00
2,807.00
235.00
377.00
111.84
28.00
53.51
180.00

This graph shows the money laundering process for five of the Evil Corp ransomware strains we mentioned above. While all of them appear to be run by separate organizations, most send funds derived from attacks to the same group of intermediary wallets, and from there move funds to many of the same deposit addresses at high-risk exchanges.

But why does Evil Corp rebrand its ransomware strains so often? Most analysts believe it's an effort to evade sanctions. Evil Corp, whose leaders are suspected to have ties to the Russian government, has been sanctioned by the United States since December 2019. In October 2020, the U.S. Treasury's Office of Foreign Asset Control (OFAC) reiterated guidance that ransomware victims who pay ransoms to sanctioned groups could face penalties. This put Evil Corp in a bad position, as it meant that many victims and their representatives would likely be reluctant to pay them following due diligence on the sanctions risk. By rebranding, Evil Corp likely believes it can fool victims into paying before researchers can discover the potential sanctions risk.

Unfortunately, rebranding appears to have worked for Evil Corp in many cases, as victims paid at least $85 million in ransoms to strains associated with the organization.

Ransomware payment value to strains associated with Evil Corp | 2016–2021



Of course, Evil Corp isn't the only organization rebranding its ransomware strains. In July 2021, the group behind the DarkSide ransomware strain began launching attacks with a very similar strain called BlackMatter. This came following DarkSide's attack on Colonial Pipeline and the FBI's subsequent seizing of most of that ransom, and it's our belief that the rebrand came in response to pressure from law enforcement. One piece of evidence supporting this is BlackMatter's stated unwillingness to attack oil and gas companies — that would make sense for a rebranded DarkSide, as the group's attack on Colonial ended poorly for them.

The uptick in ransomware rebranding is an important reminder that the ransomware ecosystem is smaller than it appears at first glance. While new strains pop up all the time, many of them are ultimately run or deployed by the same groups and individuals, all of whom are likely feeling the pressure from law enforcement's increasing efforts to prevent attacks, seize extorted funds, and arrest the individuals responsible. Rebranding is one way of evading those efforts, and suggests that investigators and cybersecurity professionals may be best served by studying ransomware attackers at the organizational level, and focusing less on the unique strains.

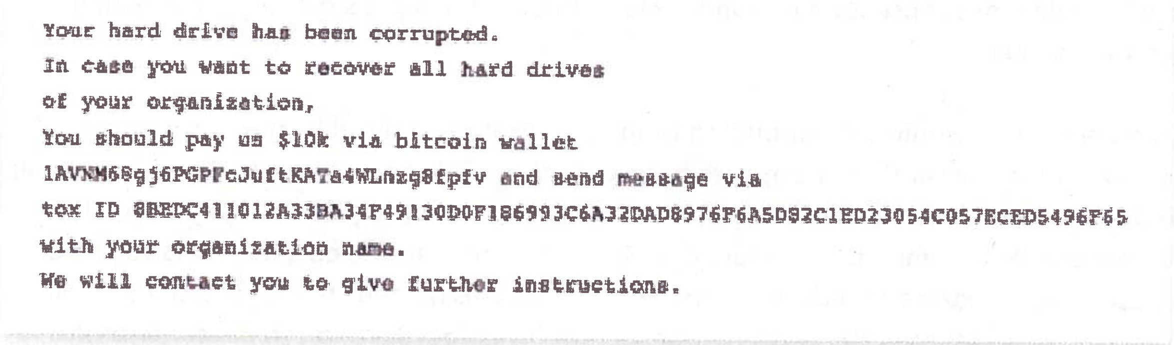
Ransomware as a geopolitical weapon

Most ransomware attacks appear to be financially motivated. However, others appear to be motivated by geopolitical goals, and seem more geared toward deception, espionage, reputational damage and disruption of the enemy government's operations.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. And that's exactly what we saw in a recent ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government.

As the Computer Emergency Response Team of Ukraine (CERT-UA) describes here, the attack occurred on the night of January 13, 2022, and disrupted several government agencies' ability to operate. The attack came against a backdrop of increasing tensions between the two countries, with Russian troop build-ups along the Ukrainian border causing concern that an invasion could be imminent. We saw a similar situation unfold in 2017, when tensions between the two nations were also running high. At that time, the Russia-based NotPetya ransomware strain, which contained no viable payment mechanism, targeted several Ukrainian organizations and was also widely judged to be a geopolitically motivated disruption attempt by the Russian military rather than a money-making effort.

Microsoft Security published its own analysis of the recent attack, noting that the ransomware strain in question — dubbed DEV-0586 or more commonly known as WhisperGate— has no way of returning victims' access to their files. Microsoft Security's blog also includes the message the ransomware group displayed to its Ukrainian victims.



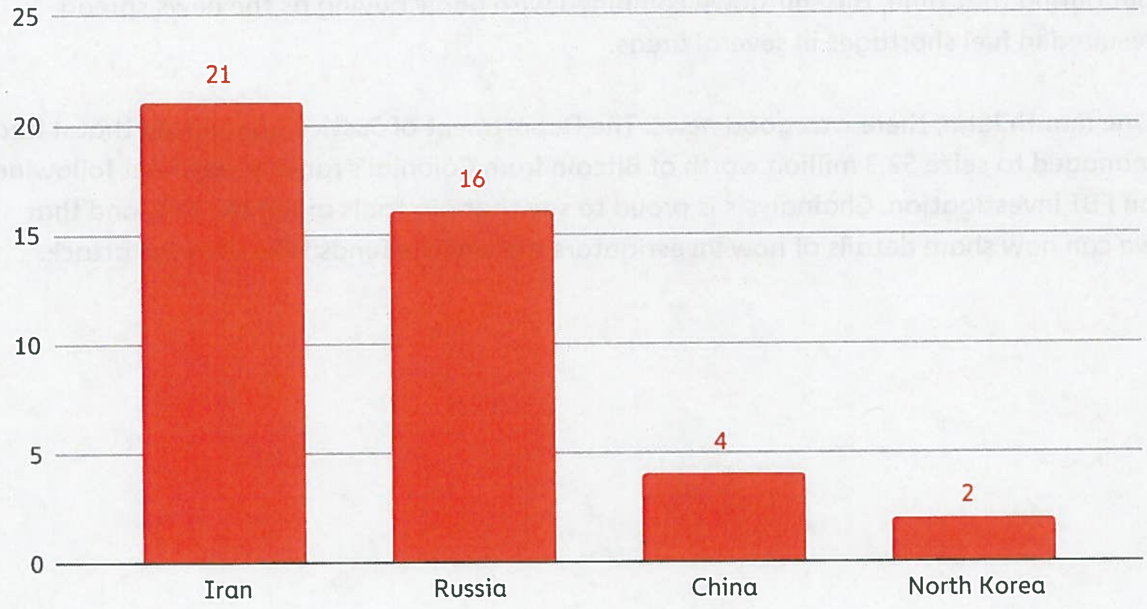
```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

Credit: Microsoft Security Blog

DEV-0586's address doesn't have an extensive transaction history for us to draw from. But further analysis of the ransomware's technical characteristics indicates even more geopolitical gamesmanship. On January 26, CERT-UA released a report showing that DEV-0586 contains code repurposed from WhiteBlackCrypt, a ransomware strain active in 2021 that, like DEV-0586, is designed to wipe victims' systems rather than extort them for money. But there's a twist: WhiteBlackCrypt targeted Russian organizations rather than Ukrainian ones. Cybersecurity analysts believe DEV-0586's reuse of code previously used by WhiteBlackCrypt, as well as the presence of other similarities linking the two strains, is a gambit by Russian hackers to make DEV-0586 appear to be of Ukrainian rather than Russian origin — in other words, a false flag attack. The gambit shows how far state actors using ransomware to attack foes will go to conceal their attacks' origins and maintain plausible deniability. We'll continue to monitor DEV-0586's address for more activity and provide updates when possible.

Russia-affiliated attackers aren't the only ones using ransomware for geopolitical ends. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, are geared more toward causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth over the last year in the number of ransomware strains attributed to Iranian cybercriminals in the past year — in fact, Iran accounts for more individual identified strains than any other country.

Number of ransomware strains with suspected links to specific countries



To be clear, many of those Iranian ransomware strains are used for conventional, financially motivated attacks by cybercriminals operating in the country. Iran has a highly educated population but limited occupational opportunities, which likely contributes to the allure of ransomware. However, other strains behave more like tools of espionage, extorting negligible amounts of cryptocurrency from victims. Other analysts have previously identified instances of strains affiliated with China, such as ColdLock, carrying out similar geopolitical attacks on Taiwanese organizations.

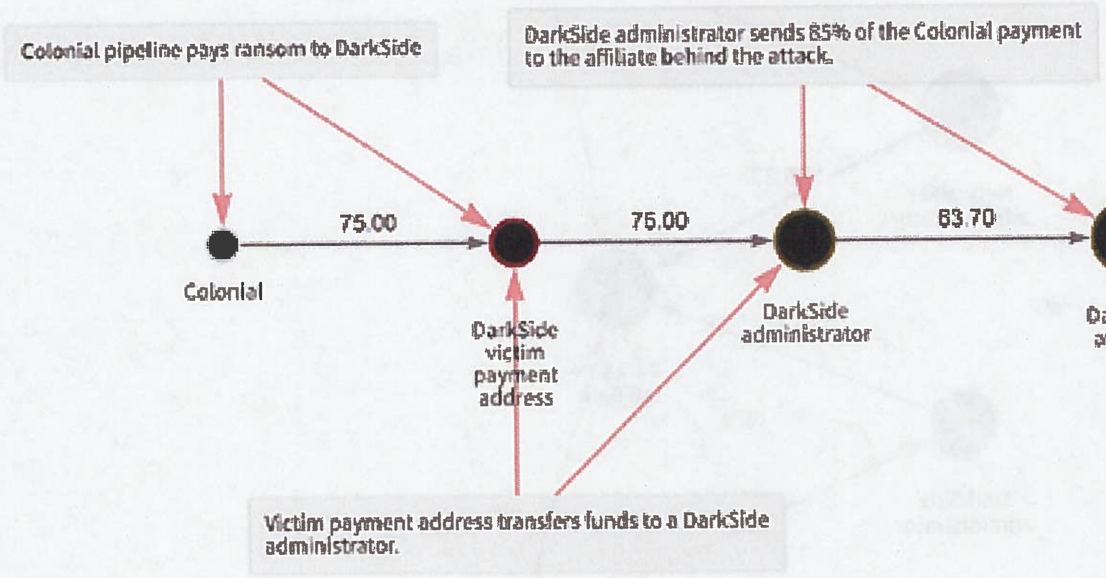
Ransomware is a useful cover for strategic denial and deception against enemy states because attacks can be carried out cheaply, and it gives the attacking nation some measure of plausible deniability, as they can always claim the attack was carried out by mere cybercriminals or another nation state. But even ransomware attacks carried out for non-financial reasons leave a trail on the blockchain. For that reason, it's crucial that agencies focused on national security understand how to trace funds using blockchain analysis, as this is the key to identifying the individuals involved in the attacks themselves, the tools they use, and how they launder any funds obtained from victims.

Chainalysis in action: How FBI investigators tracked and seized funds from DarkSide following the Colonial Pipeline ransomware attack

On May 7, 2021, Colonial Pipeline, an oil pipeline company that supplies energy to the southeastern United States, fell victim to a ransomware attack, forcing it to temporarily cease operations. Within hours of the attack, Colonial paid a ransom of 75 Bitcoin — worth roughly $4.4 million at the time — to DarkSide, the Russia-based cybercriminal group responsible for the attack. Six days later, Colonial was able to resume operations, but during that time, the shutdown combined with panic buying as the news spread resulted in fuel shortages in several areas.

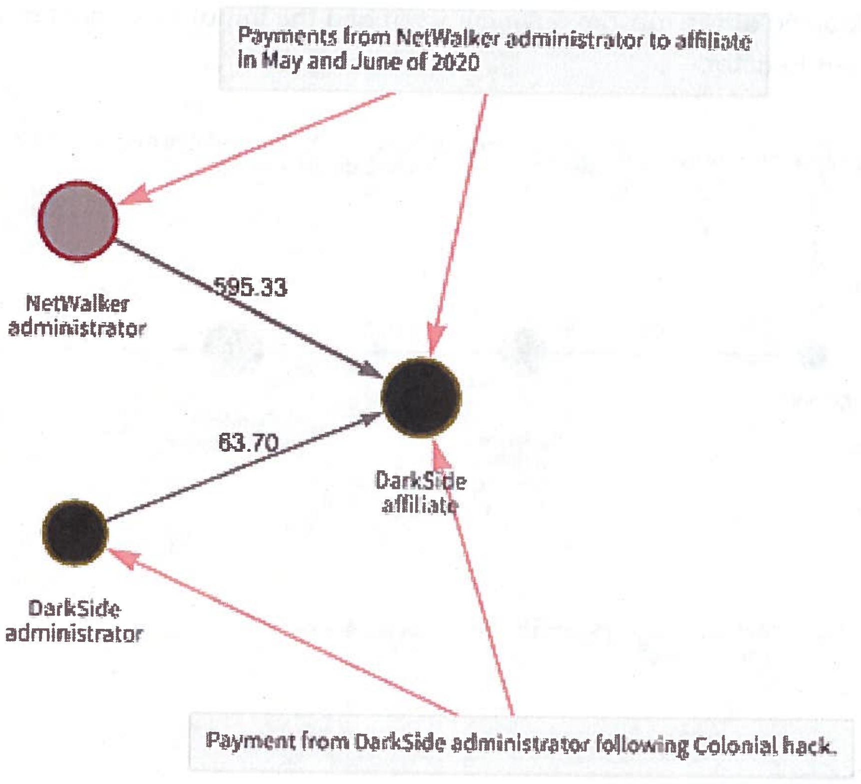
One month later, there was good news: The Department of Justice announced that it had managed to seize $2.3 million worth of Bitcoin from Colonial's ransom payment following an FBI investigation. Chainalysis is proud to say that our tools aided the FBI, and that we can now share details of how investigators tracked the funds following the attack.

Let's start by looking at the ransom payment itself and the initial movement of funds using Chainalysis Reactor.


Colonial pipeline pays ransom to DarkSide
DarkSide administrator sends 85% of the Colonial payment to the affiliate behind the attack.
75.00
75.00
63.70
Colonial
DarkSide victim payment address
DarkSide administrator
DarkSide affiliate
Victim payment address transfers funds to a DarkSide administrator.

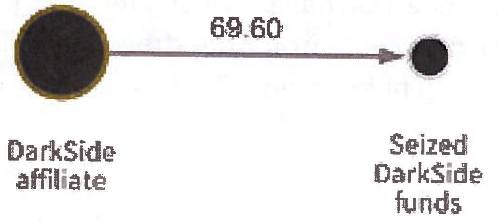
First, on the left, we see the initial payment of 75 Bitcoin from Colonial to the address provided by the attackers. Soon after, that address transferred the funds to an address controlled by DarkSide's administrators, who then sent 63.7 Bitcoin — 85% of Colonial's payment — to the affiliate who controlled the attack. That point is key — DarkSide operates on the Ransomware as a Service (RaaS) model, meaning the affiliates who carry out the attack effectively "rent" usage of DarkSide's technology from the core group of administrators who created and manage the ransomware strain itself. Administrators take a small cut of the payment from each successful attack in return, as we see above.

Interestingly, the affiliate in question had previously received payments from addresses associated with NetWalker, another ransomware strain operating on the RaaS model that was disrupted by law enforcement in January 2021.


Payments from NetWalker administrator to affiliate in May and June of 2020
595.33
NetWalker administrator
63.70
DarkSide affiliate
DarkSide administrator
Payment from DarkSide administrator following Colonial hack.

The affiliate received a total of 595.3 Bitcoin from the NetWalker administrator in a series of four payments in late May and early June of 2020, suggesting that they may have also carried out attacks for that strain as well. This wouldn't be surprising, as we've noted other instances of affiliate overlap between ransomware strains in the past.

After tracking the funds to the affiliate's address, FBI investigators were able to seize the funds on May 28, 2021.



The seizure represents a huge step forward in the fight against ransomware, and especially ransomware strains that attack our critical infrastructure. We continue to monitor the movement of funds using our tools so that we can provide helpful insight to authorities as they investigate further and, hopefully, seize the remainder of the funds.

What's next for ransomware?

Ransomware isn't just dangerous. It's also one of the most dynamic, constantly changing forms of cryptocurrency-based crime. Between constant rebrands, shifting money laundering strategies, and the influence of geopolitics, it's hard to know what's coming next. One trend to look out for though is Monero ransoms. Analysts have noted that more and more attackers are demanding victims pay in Monero, likely due to the heightened anonymity it offers. While the vast majority of attackers continue to demand Bitcoin, law enforcement and cybersecurity professionals should keep an eye out for ransom notes requesting Monero or assets associated with other protocols with privacy-enhancing features, as this will change the investigative tactics they must employ.

There's only one thing that's certain in ransomware: Law enforcement will continue to investigate the cybercriminals responsible, and Chainalysis software and services will be there to help them every step of the way. Events like the seizure of funds from DarkSide show that we're making progress, and we look forward to keeping up the fight in 2022.

Malware

Meet the Malware Families Helping Hackers Steal and Mine Millions in Cryptocurrency

When it comes to cryptocurrency theft, industry observers tend to focus on attacks against large organizations — namely hacks of cryptocurrency exchanges or ransomware attacks against critical infrastructure. But over the last few years, we've observed hackers using malware to steal smaller amounts of cryptocurrency from individual users.

Using malware to steal or extort cryptocurrency is nothing new. In fact, nearly all ransomware strains are initially delivered to victims' devices through malware, and many large-scale exchange hacks also involve malware. But these attacks take careful planning and skill to pull off, as they're typically targeted against deep-pocketed, professional organizations and, if successful, require hackers to launder large sums of cryptocurrency. With other types of malware, less sophisticated hackers can take a cheaper "spray-and-pray" approach, spamming millions of potential victims and stealing smaller amounts from each individual tricked into downloading the malware. Many of these malware strains are available for purchase on the darknet, making it even easier for less sophisticated hackers to deploy them against victims.

We're equipping our partners in law enforcement, compliance, and cybersecurity to combat this problem by adding a new tag for malware operator addresses in all Chainalysis products. Below, we'll examine trends in hackers' usage of cryptocurrency-focused malware over the last decade and share two case studies to help you understand this under-discussed area of crypto crime.

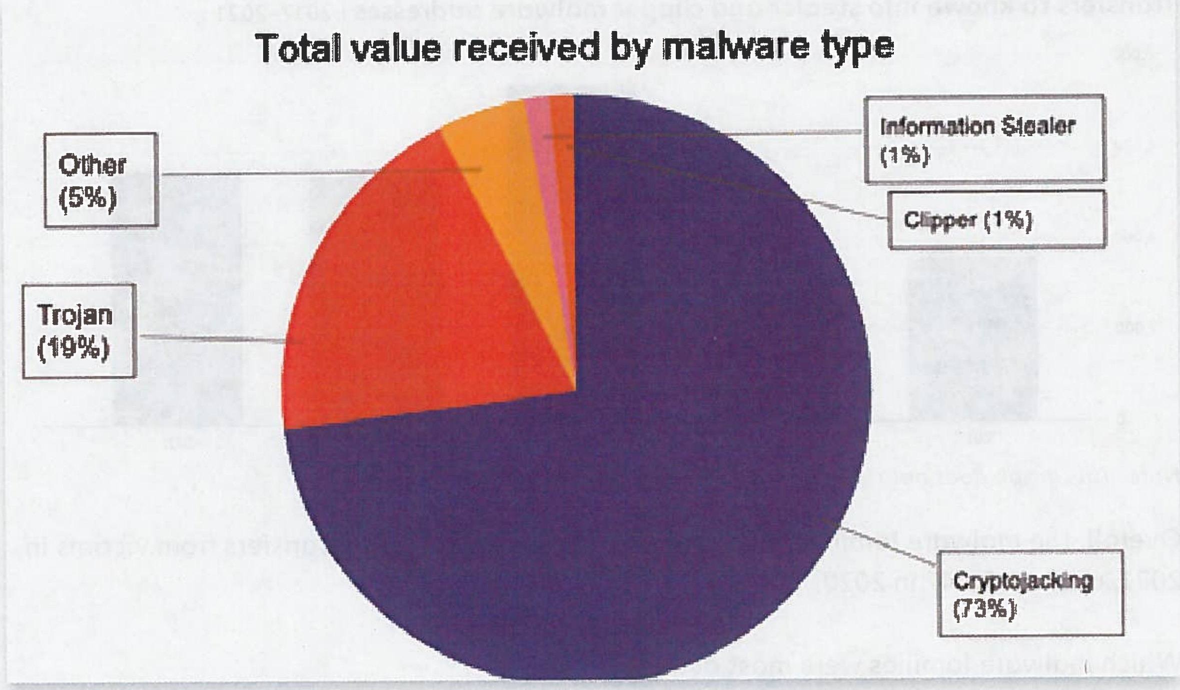
Malware and cryptocurrency summarized

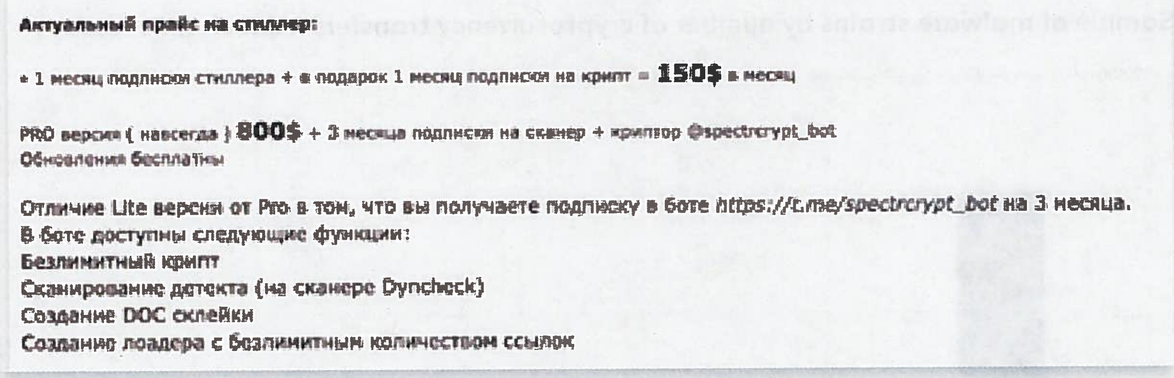
Malware refers to malicious software that carries out harmful activity on a victim's device, usually without their knowledge. Malware-powered crime can be as simple as stealing information or money from victims, but can also be much more complex and grand in scale. For instance, malware operators who have infected enough devices can use those devices as a botnet, having them work in concert to carry out distributed denial-of-service (DDOS) attacks, commit ad fraud, or send spam emails to spread the malware further.

The malware families we discuss here are all used to steal cryptocurrency from victims, though some of them are used for other activities as well. The grid below breaks down the most common types of cryptocurrency-focused malware families.

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and cryptocurrency wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace cryptocurrency addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine cryptocurrency.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

Many of the malware families described above are available to purchase for relatively little money on cybercriminal forums. For instance, the screenshots below show an advertisement for Redline, an info stealer malware, posted on a Russian cybercrime forum.





Актуальный прайс на стиллер:

• 1 месяц подписки стиллера + в подарок 1 месяц подписки на крипт = **150$** в месяц

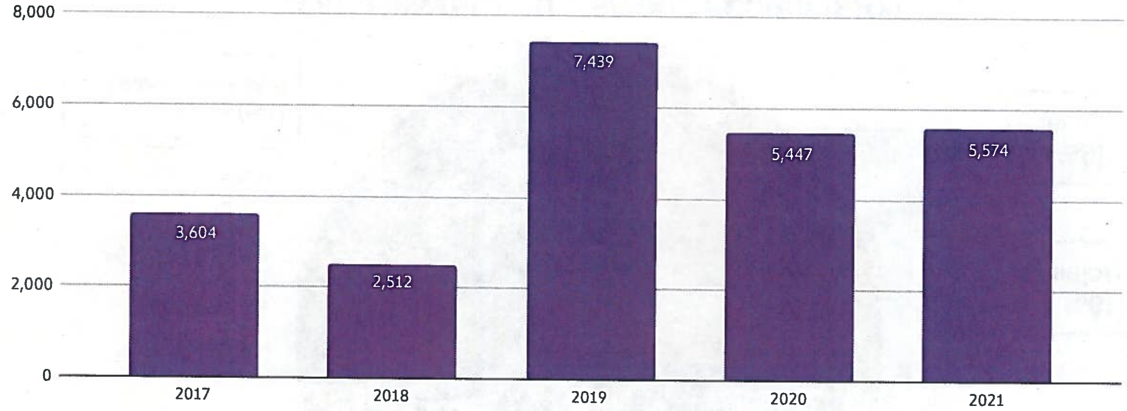
PRO версия (навсегда) **800$** + 3 месяца подписки на сканер + криптор @spectrcrypt_bot
Обновления бесплатны

Отличие Lite версии от Pro в том, что вы получаете подписку в боте *https://t.me/spectrcrypt_bot* на 3 месяца.
В боте доступны следующие функции:
Безлимитный крипт
Сканирование детекта (на сканере Dyncheck)
Создание DOC склейки
Создание лоадера с безлимитным количеством ссылок

The seller offers cybercriminals one month of Redline access for $150 and lifetime access for $800. Buyers also get access to Spectrum Crypt Service, a Telegram-based tool that allows cybercriminals to encrypt Redline so that it's more difficult for victims' antivirus software to detect it once it's been downloaded. The proliferation of cheap access to malware families like Redline means that even relatively low-skilled cybercriminals can use them to steal cryptocurrency. Law enforcement and compliance teams must keep this in mind, and understand that the malware attacks they investigate aren't necessarily carried out by the administrators of the malware family itself, but instead are often carried out by smaller groups renting access to the malware family, similar to ransomware affiliates.

The graph below shows the number of victim transfers to cryptocurrency addresses associated with a sample of malware families in the info stealer and clipper categories investigated by Chainalysis.

Transfers to known info stealer and clipper malware addresses | 2017–2021

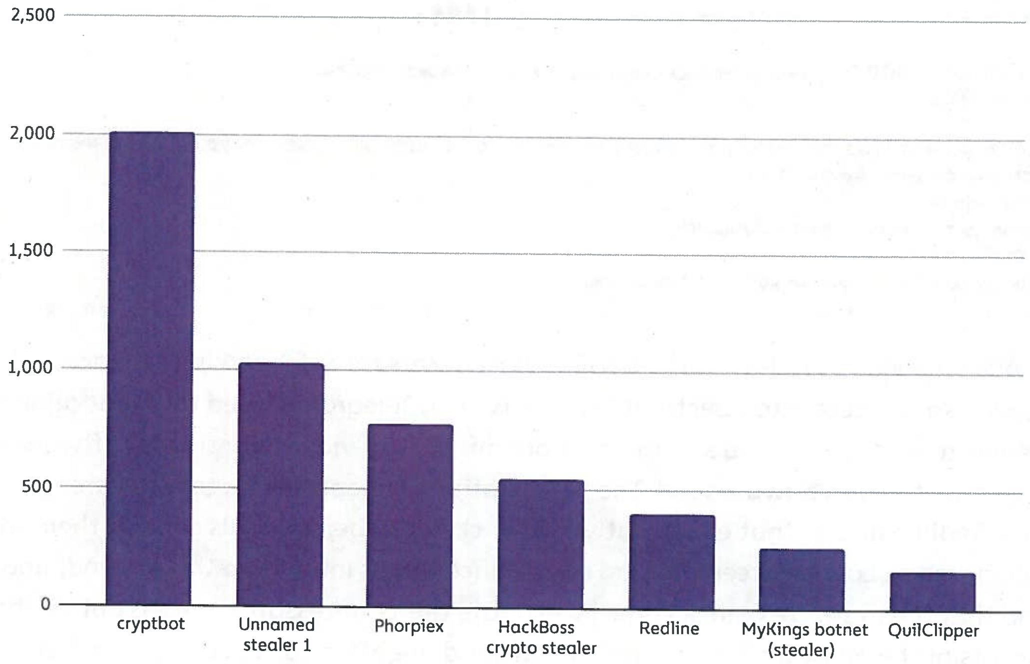


Note: This graph does not reflect activity by cryptojackers or ransomware.

Overall, the malware families in this sample have received 5,574 transfers from victims in 2021, up from 5,447 in 2020.

Which malware families were most active?

Sample of malware strains by number of cryptocurrency transfers from victims | 2021



Note: This graph does not reflect activity by cryptojackers or ransomware.

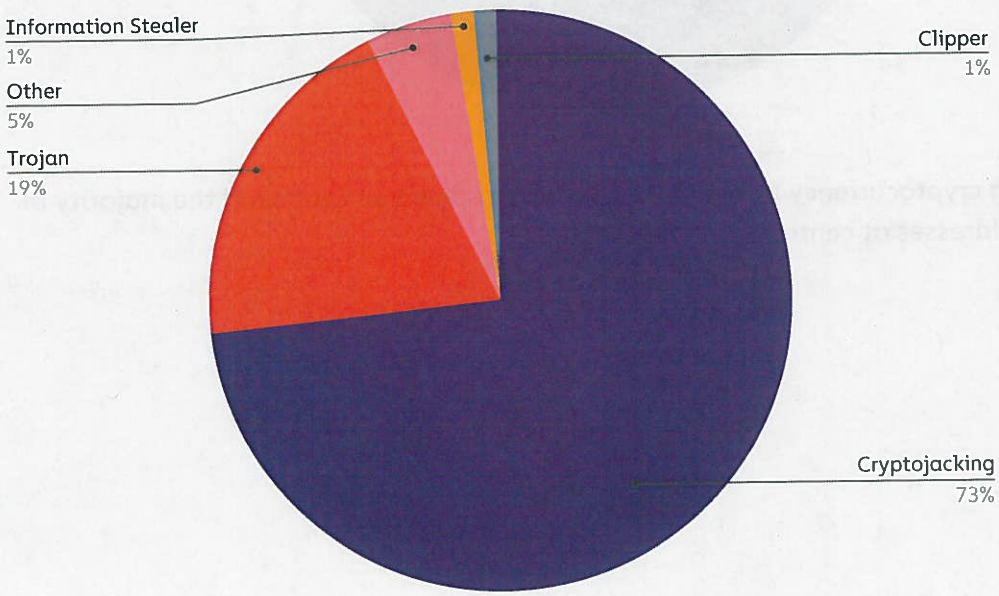
Cryptbot, an infostealer that takes victims' cryptocurrency wallet and account credentials, was the most prolific malware family in the group, raking in almost half a million dollars in pilfered Bitcoin. Another prolific family is QuilClipper, a clipboard stealer or "clipper," ranked eighth on the graph above. Clippers can be used to insert new text into the "clipboard" that holds text a user has copied, usually with the intent to paste elsewhere. Clippers typically use this functionality to detect when a user has copied a cryptocurrency address to which they intend to send funds — the clipper malware effectively hijacks the transaction by then substituting an address controlled by the hacker for the one copied by the user, thereby tricking the user into sending cryptocurrency to the hacker.

However, none of those numbers reflect totals from what we believe to be the most prolific type of cryptocurrency-focused malware: Cryptojackers.

Cryptojacker activity is murky but substantial

Cryptojackers obtain funds for malware operators by utilizing the victim's computing power to mine cryptocurrency — usually Monero, but we've seen Zcash and Ethereum mined as well. Since funds are moving directly from the mempool to mining addresses unknown to us, rather than from the victim's wallet to a new wallet, it's more difficult to passively collect data on cryptojacking activity the way we can other forms of cryptocurrency-based crime. However, we know it's a big problem. In 2020, Cisco's cloud security division reported that cryptojacking malware affected 69% of its clients, which would translate to an incredible amount of stolen computer power, and therefore a significant amount of illicitly-mined cryptocurrency. A 2018 report from Palo Alto Networks estimated that 5% of all Monero in circulation was mined by cryptojackers, which would represent over $100 million in revenue, making cryptojackers the most prolific form of cryptocurrency-focused malware.

Total value received by malware type

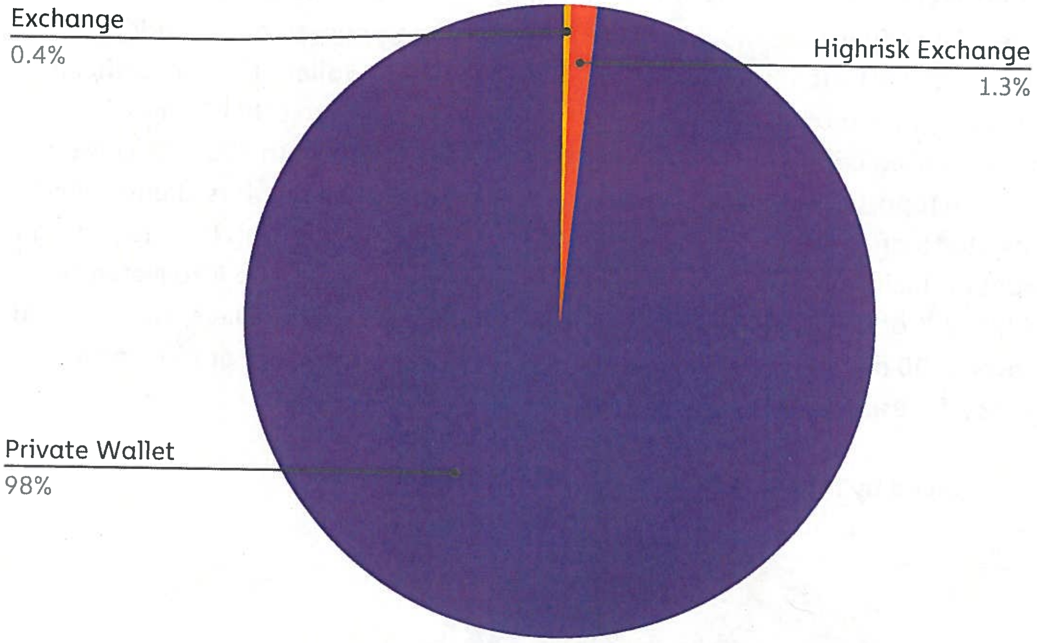


These numbers are likely only scratching the surface for cryptojacking. As we identify more malware families involved in this activity, we expect to learn that total revenue for the category is even bigger than it currently appears.

Malware and money laundering

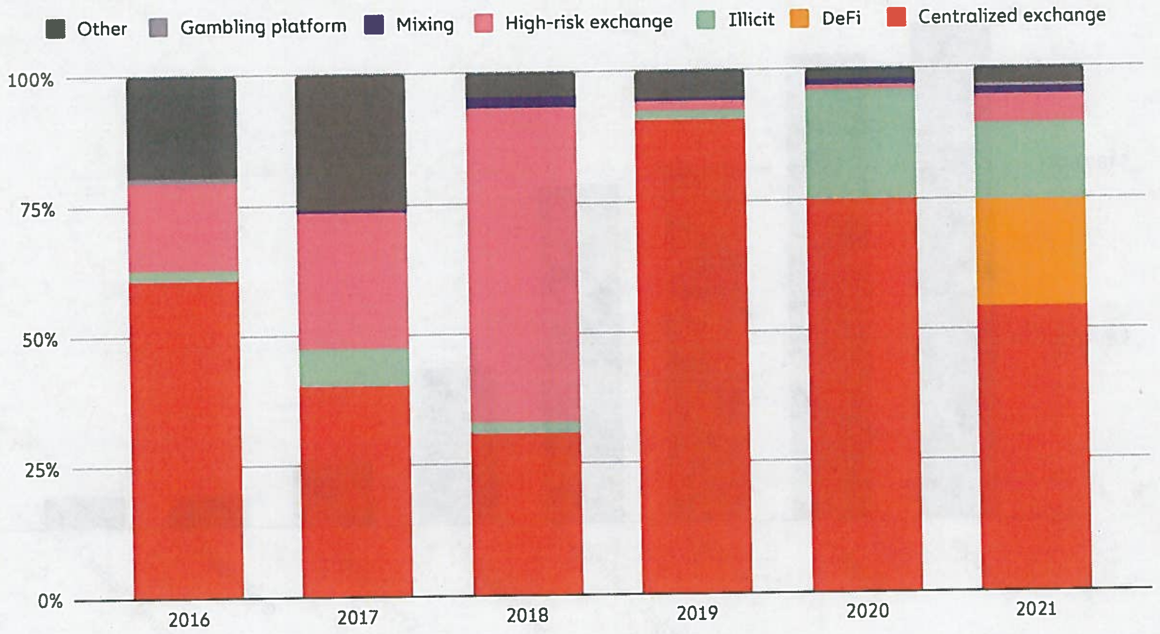
The vast majority of malware operators receive initial victim payments at private wallet addresses, though a few use addresses hosted by larger services. Of that smaller group, the majority use addresses hosted by exchanges — mostly high-risk exchanges that have low or no KYC (Know Your Customer) requirements.

Malware operator addresses by hosting platform



After receiving cryptocurrency from victims, malware operators then send the majority of funds on to addresses at centralized exchanges.

Destination of funds leaving malware family addresses | 2016–2021



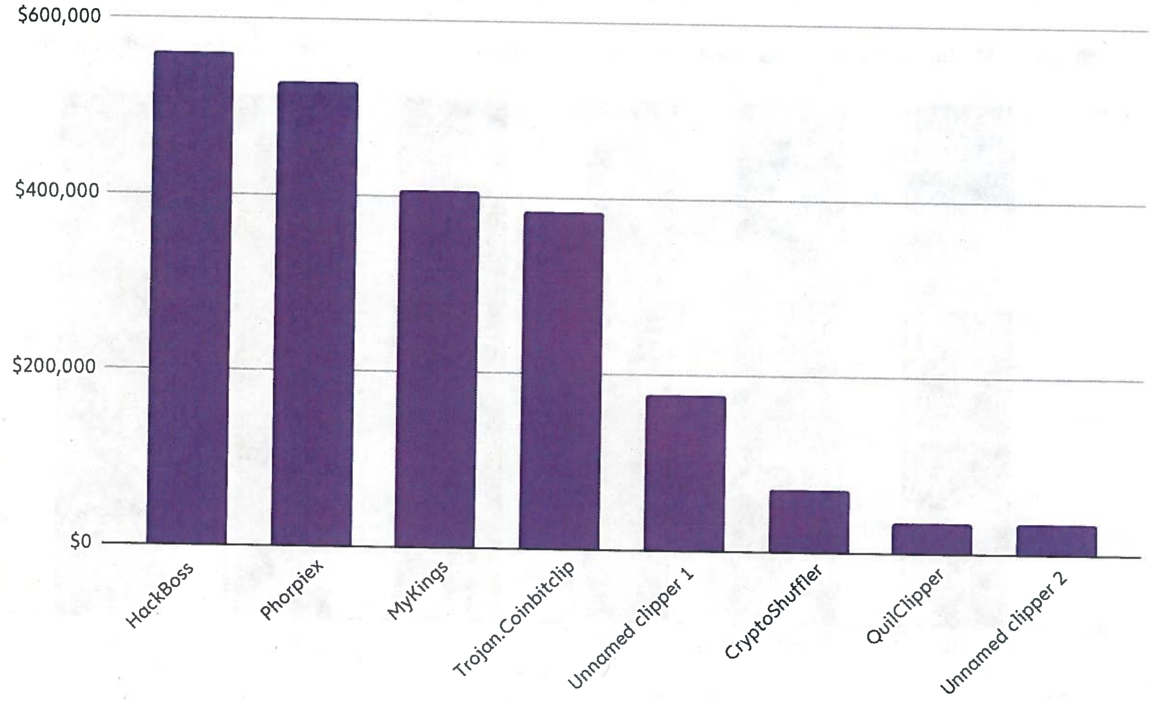
However, that majority is slim and getting slimmer. Exchanges only received 54% of funds sent from malware addresses in 2021, down from 75% in 2020. DeFi protocols make up much of the difference at 20% in 2021, after having received a negligible share of malware funds in 2020. Illicit services seemingly unrelated to malware — mostly darknet markets — are also a significant money laundering avenue for malware operators, having received roughly 15% of all funds sent from malware addresses in 2021.

Malware-based cryptocurrency theft is difficult to investigate in part due to the large number of less sophisticated cybercriminals who can rent access to these malware families. But studying how cybercriminals launder stolen cryptocurrency may be investigators' best bet for finding those involved. Using blockchain analysis, investigators can follow the funds, find the deposit addresses cybercriminals use to cash out, and subpoena the services hosting those addresses to identify the attackers.

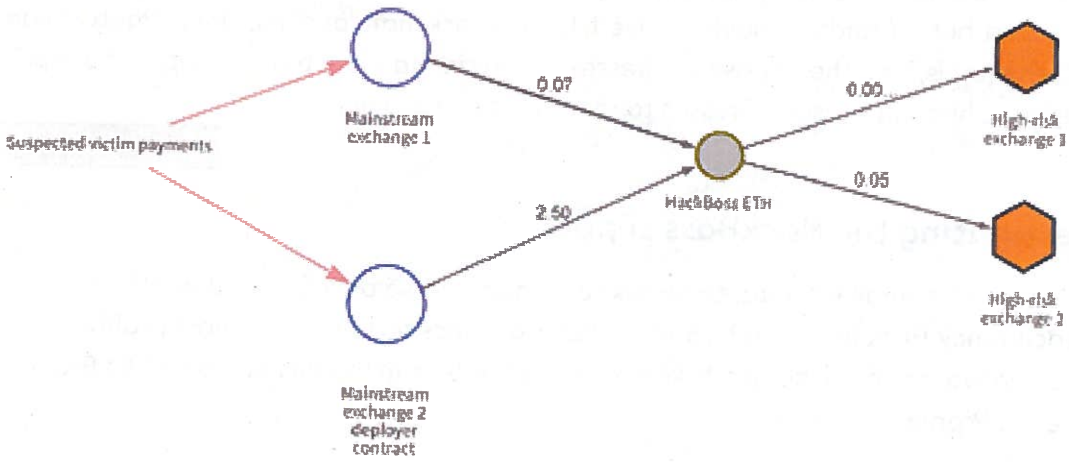
Investigating the HackBoss clipper

According to Chainalysis data, the HackBoss clipper stole over $80,000 worth of cryptocurrency throughout 2021. Since 2012, HackBoss has been the most prolific clipper malware overall, having taken over $560,000 from victims in assets like Bitcoin, Ethereum, Ripple, and more.

Clipper malware families by all-time revenue



Interestingly, HackBoss is targeted at fellow hackers rather than what we think of as ordinary victims. According to reporting from Avast.io's Decoded, HackBoss is distributed through a Telegram channel that purports to provide hacking tools such as social media site crackers. However, instead of those tools, the channel's users are actually downloading the HackBoss clipper, which steals cryptocurrency from them by inserting its own addresses into the clipboard when victims attempt to copy and paste another address to carry out a cryptocurrency transaction.



The Chainalysis Reactor graph above shows HackBoss receiving cryptocurrency from victims on the left. From there, the malware operators move funds to deposit addresses hosted by high-risk exchanges.

While HackBoss is uniquely targeted at hackers attempting to download tools to carry out their own cybercrimes, most other clippers are targeted at ordinary cryptocurrency users. It's extremely difficult to know if one has fallen victim to a clipper until a transaction has been hijacked given how long and complex cryptocurrency addresses are — most people don't read through the recipient's entire address between pasting it into their wallet and sending a transaction. However, that may be necessary for users trying to be as careful as possible. At the very least, cryptocurrency users need to be vigilant about what links they click and programs they download, as there are several active malware strains — not just clippers, but others too — attempting to steal their funds.

Case study: Glupteba botnet hijacks computers to mine Monero and harnesses the Bitcoin blockchain to evade shutdown

A complaint filed by Google in late 2021 named multiple Russian nationals and entities alleged to be responsible for operating the Glupteba botnet, which has compromised over 1 million machines. Glupteba's operators have used these machines for several criminal schemes, including utilizing their computing power to mine cryptocurrency — specifically, in this case, Monero — in a practice known as cryptojacking.

Perhaps most notable is Glupteba's use of the Bitcoin blockchain to withstand attempts to take it offline, encoding updated command-and-control servers (C2) into the Op_Returns of Bitcoin transactions. Google used Chainalysis software and Chainalysis Investigative Services to analyze the Bitcoin addresses and transactions responsible for sending updated C2 instructions. Below, we'll break down how the Glupteba botnet uses the Bitcoin blockchain to defend itself and what it means for cybersecurity and law enforcement.

A primer on the Glupteba botnet

The cybercriminals behind the Glupteba botnet have used it to carry out a variety of criminal schemes. In addition to cryptojacking, the botnet has been used to acquire and sell Google account information stolen from infected machines, commit digital advertising fraud, and sell stolen credit card data.

Google was able to identify the individuals named in the complaint by obtaining and examining an IP address used by one of Glupteba's C2 servers. All individuals were also listed as owners or administrators of shell companies connected to Glupteba-related crimes, such as one used to sell fraudulent digital advertising impressions supplied by the botnet. Google was able to successfully take down the current C2 server, however as Glupteba has proven to be infallible against these actions through it's blockchain failsafe, we will soon see a new C2 assigned.

How Glupteba weaponizes the blockchain

In order to direct botnets, cybercriminals rely on command-and-control (C2) servers, which allow them to send commands to machines infected with malware. Botnets look for domain addresses controlled by their C2 servers in order to receive instructions, with directions on where to look for those domain addresses hard coded into the malware itself.

In order to combat botnets, law enforcement and cybersecurity professionals try to take those domains offline so that the botnets can no longer receive instructions from the C2 server. In response, botnet operators typically set up a number of backup domains in case the active domain is taken down. Most malware algorithmically generates new domain addresses for botnets to scan until they find one of those backups, allowing them to receive new instructions from the C2 server.

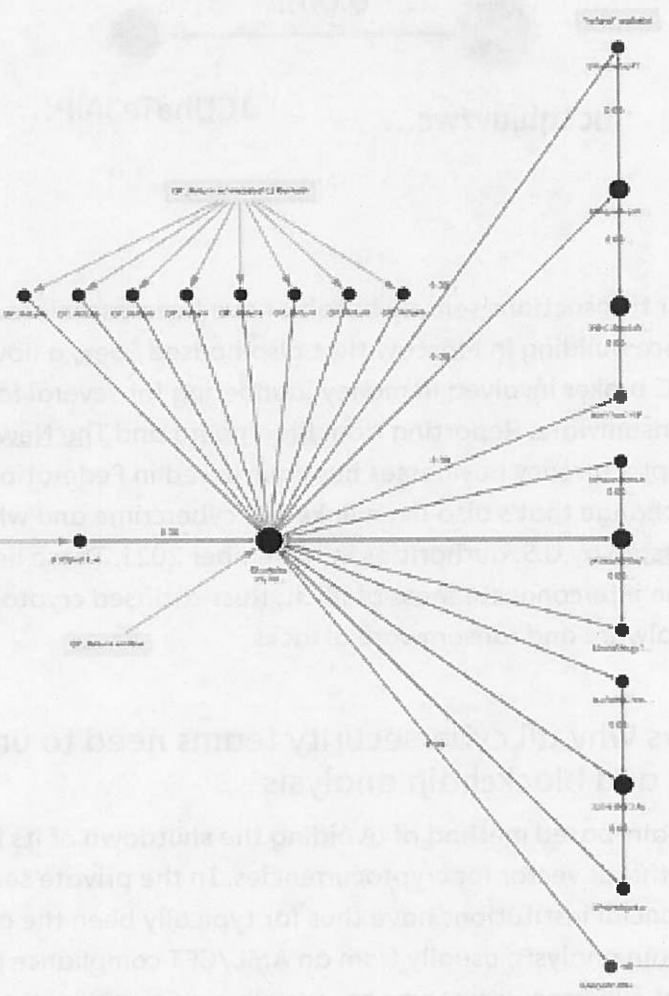
However, Glupteba does something new. When its C2 server is disrupted, Glupteba is programmed to search the Bitcoin blockchain for transactions carried out by three addresses controlled by its operators. Those addresses carry out transactions of little or no monetary value, with encrypted data written into the transaction's Op_Return field, which is used to mark transactions as invalid. Glupteba malware can then decode the data entered into the Op_Return field to obtain the domain address of a new C2 server.

In other words, whenever one of Glupteba's C2 servers is shut down, it can simply scan the blockchain to find the new C2 server domain address, hidden amongst hundreds of thousands of daily transactions. This tactic makes the Glupteba botnet extremely difficult to disrupt through conventional cybersecurity techniques focused on disabling C2 server domains. This is the first known case of a botnet using this approach.

Here's what we know about the three Bitcoin addresses we've identified as being used by Glupteba's operators to keep the botnet online:

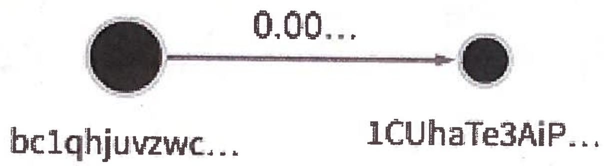
Address	Dates active	Number of transfers	Number of Op_Returns
15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6	6/17/2019 - 5/13/2020	32	8
1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1	4/8/2020 - 10/19/2021	16	6
1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97	10/13/21 - present	18	6

Combined, the three addresses have only transacted a few hundred dollars' worth of Bitcoin, but the messages encoded into the Op_Returns on some of those transactions have helped the Glupteba botnet remain operational. Let's look more closely at address 157d... in Chainalysis Reactor as an example.



We see that the Glupteba address received its initial funding from a mixing service, before initiating the invalid transactions with Op_Returns we see at the top of the graph. The funds associated with those invalid transactions then travel to the refund wallets on the right, and eventually back to the original Glupteba address. The other two addresses show similar transaction patterns. Google identified the three Glupteba addresses and brought them to Chainalysis, at which point our investigators were able to decode the data contained in the Op_Returns' message fields, allowing them to discover the new C2 server domain addresses being sent to the botnet.

Like address 15y7d..., address 1CgPC... was initially funded through outputs from mixing transactions. However, the third address, 1Cuha..., received initial funding from another private wallet address: bc1qhjuvzwcv0pp68kn2sqvx3d2k3pqfllv3c4vywd.



Interestingly, other transactions sent by bc1qh... have been associated with Federation Tower, a luxury office building in Moscow that also housed Suex, a now-sanctioned cryptocurrency OTC broker involved in money laundering for several forms of cyber-crime, including ransomware. Reporting from Bloomberg and The New York Times discusses other cryptocurrency businesses headquartered in Federation Tower, including EggChange, an exchange that's also been linked to cybercrime and whose founder, Denis Dubnikov, was arrested by U.S. authorities in November 2021. These links raise more questions about the interconnectedness of illicit, Russia-based cryptocurrency businesses associated with malware and ransomware attacks.

Glupteba shows why all cybersecurity teams need to understand cryptocurrency and blockchain analysis

Glupteba's blockchain-based method of avoiding the shutdown of its botnet represents a never-before-seen threat vector for cryptocurrencies. In the private sector, cryptocurrency businesses and financial institutions have thus far typically been the ones tackling cases involved in blockchain analysis, usually from an AML/CFT compliance perspective. But this case shows that cybersecurity teams at virtually any company that could be a target for cybercriminals — especially those possessing large amounts of sensitive customer data — must be well-versed in cryptocurrency and blockchain analysis in order to stay ahead of cybercriminals. At Chainalysis, we're eager to work with those teams to help them understand how our tools can assist them in diagnosing and fighting these threats, so that cryptocurrencies can't be weaponized against them or their users.

The convergence of malware and cryptocurrency: Same cybercriminals, new methods

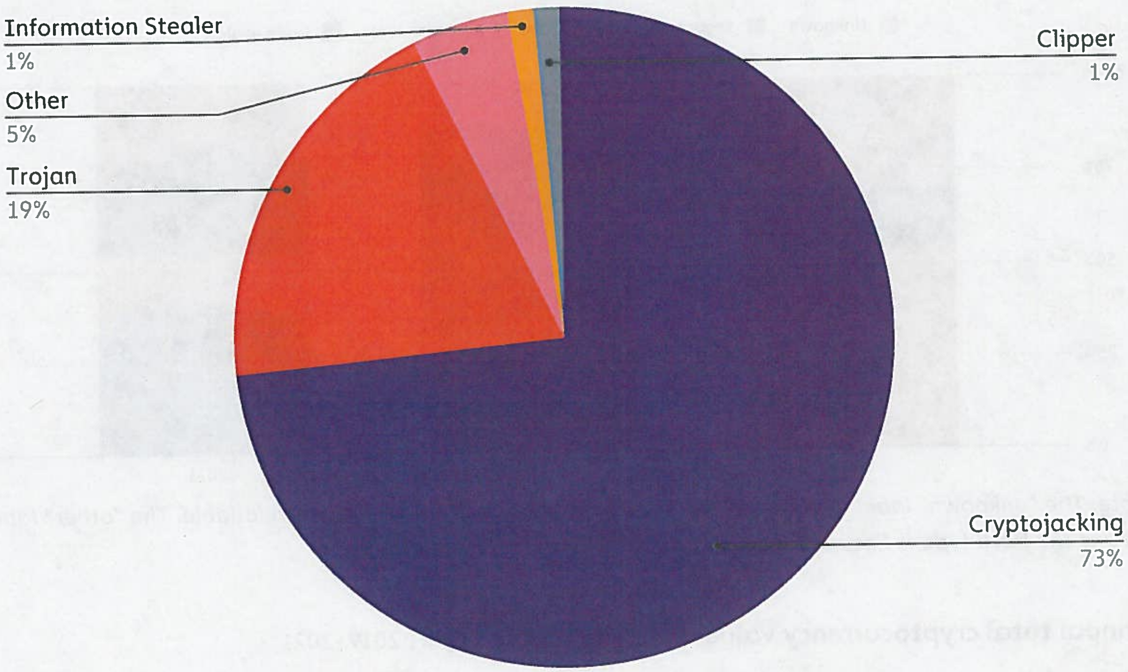
The cybersecurity industry has been dealing with malware for years, but the usage of these malicious programs to steal cryptocurrency means cybersecurity teams need new tools in their toolbox. Chainalysis gives cybersecurity teams new avenues of investigation for malware, allowing them to take advantage of blockchains' transparency and track the movement of funds that have been stolen until they reach an address whose owner can be identified. Likewise, cryptocurrency compliance teams already well-versed in blockchain analysis must educate themselves on malware in order to ensure these threat actors aren't taking advantage of their platforms to launder stolen cryptocurrency.

Stolen Funds

More Than $3 Billion Stolen in 2021 As DeFi Thefts Leap 1,330%

2021 was a big year for digital thieves. Throughout the year, $3.2 billion in cryptocurrency was stolen from individuals and services — almost 6x the amount stolen in 2020.

Total value stolen and total number of thefts | 2015–2021



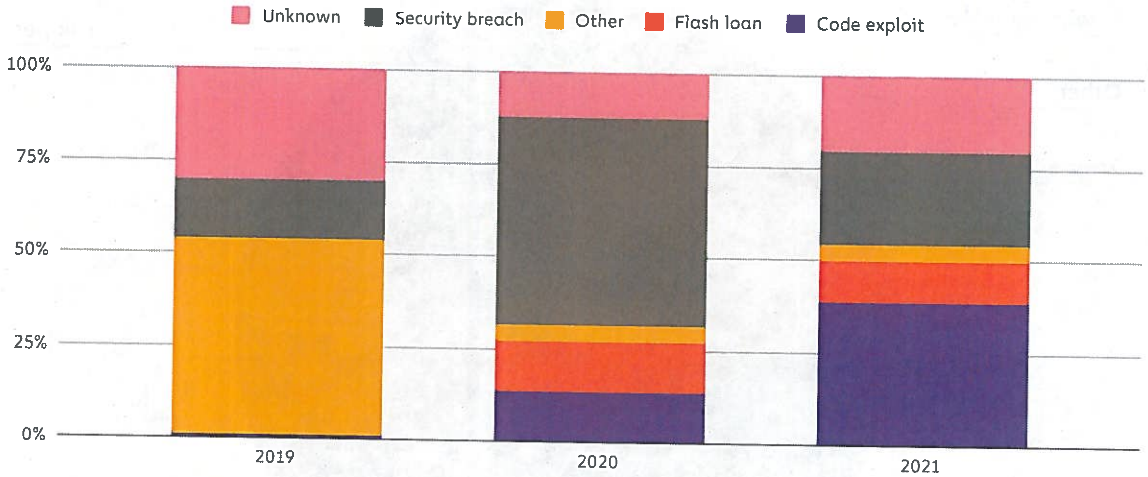
And that's just part of the story: Approximately $2.3 billion of those funds were stolen from DeFi platforms in particular, and the value stolen from these protocols catapulted 1,330%.

This shift toward DeFi-centric attacks doesn't just sound pronounced—it looks like it, too. In every year prior to 2021, centralized exchanges lost the most cryptocurrency to theft by a large margin. But this year, DeFi platform thefts dwarfed exchange thefts by a factor of six.

Code exploits are a prominent feature in 2021's cryptocurrency theft landscape

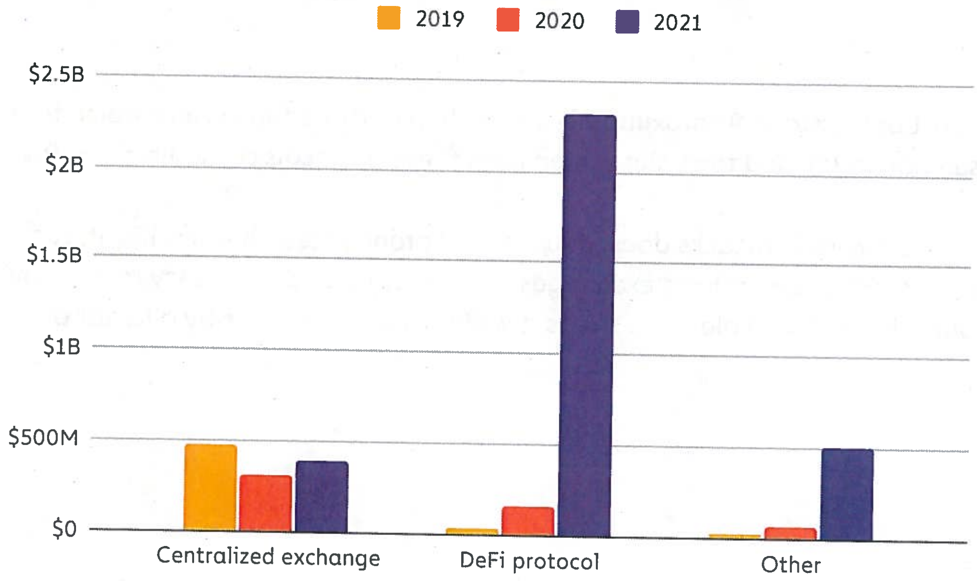
Historically, cryptocurrency thefts have largely been the result of security breaches in which hackers gain access to victims' private keys — the crypto-equivalent of pickpocketing. These keys could be acquired through phishing, keylogging, social engineering, or other techniques. From 2019 to 2021, almost 30% of all value was stolen from just this type of hack.

Total value stolen by type of attack | 2019–2021



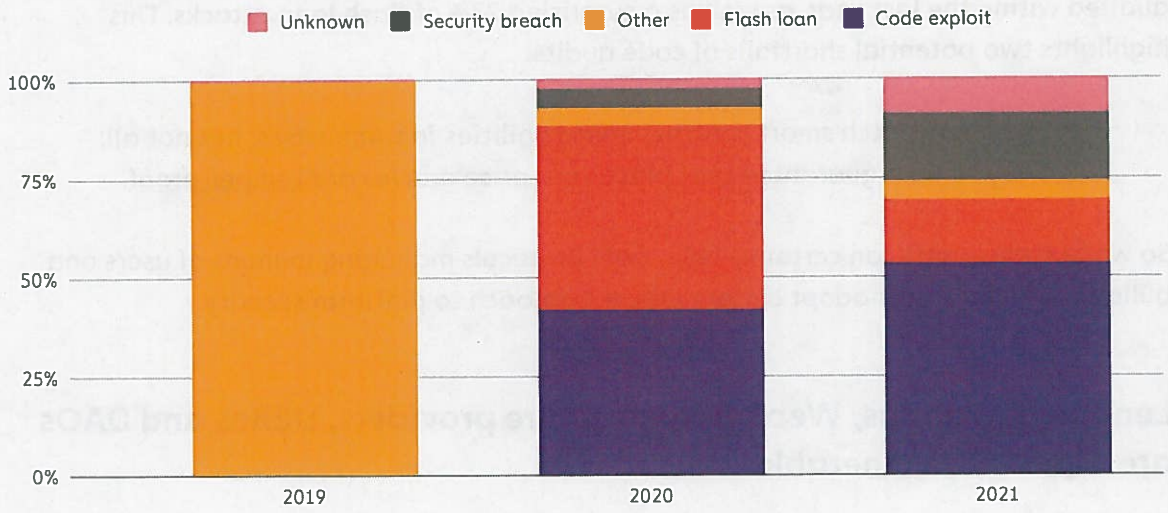
Note: The "unknown" label means information about hack type is not publicly available. The "other" label means the hack type is known but does not fit within our defined categories.

Annual total cryptocurrency value stolen by victim type | 2019–2021



But with the rise of DeFi and the extensive smart contract capabilities that power those platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.

Total value stolen from DeFi protocols by attack type | 2019–2021



These exploits occur for a variety of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and broadly positive trend: since DeFi protocols move funds without human intervention, users need to be able to audit the underlying code in order to trust the platform. But this also stands to benefit cybercriminals, who can analyze the scripts for vulnerabilities and plan exploits in advance.

Another potential point of failure is DeFi platforms' reliance on price oracles. Price oracles are tasked with maintaining accurate asset pricing data for all cryptocurrencies on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a vulnerability in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in just one night.

These two dangers—inaccurate oracles and exploitable code—underscore the need for the security of both. Fortunately, there are solutions. To ensure pricing accuracy, decentralized price oracles like Chainlink can protect platforms against price manipulation attacks. To ensure the security of smart contracts, code audits can steel programs against common hacks like reentrancy, unhandled exceptions, and transaction order dependency.

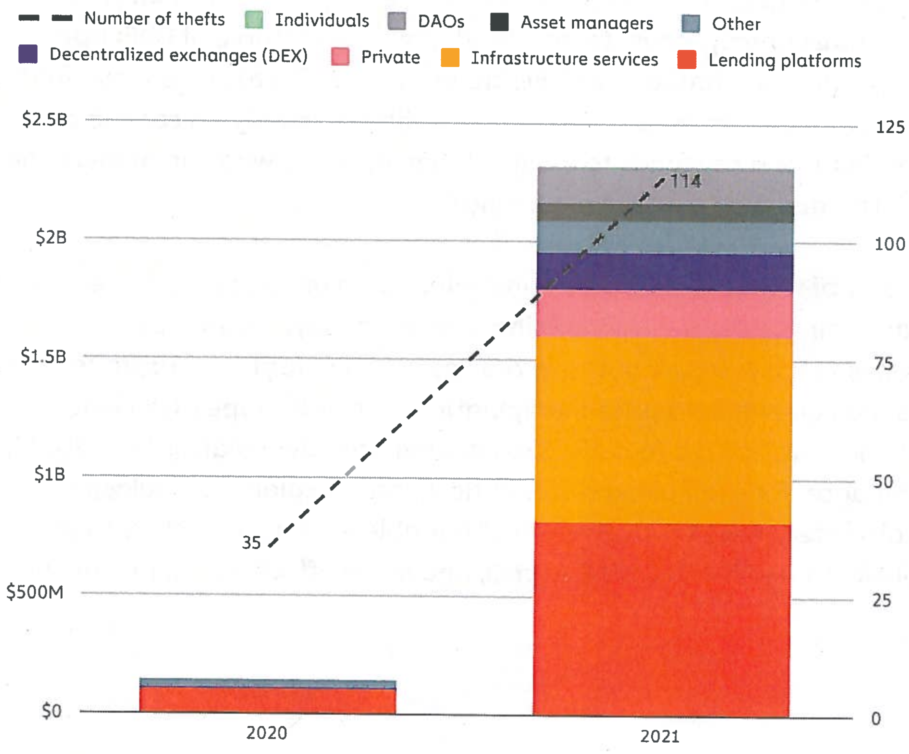
But code audits aren't infallible. Nearly 30% of code exploits occurred on platforms audited within the last year, as well as a surprising 73% of flash loan attacks. This highlights two potential shortfalls of code audits:

1. They may patch smart contract vulnerabilities *in some cases*, but not all;
2. They seldom guarantee that platforms' price oracles are tamper-proof.

So while code audits can certainly help, DeFi protocols managing millions of users and billions of dollars must adopt a more robust approach to platform security.

Lending platforms, Web3 infrastructure providers, DEXes and DAOs are especially vulnerable

DeFi-related theft losses vs. number of theft incidents | 2020–2021

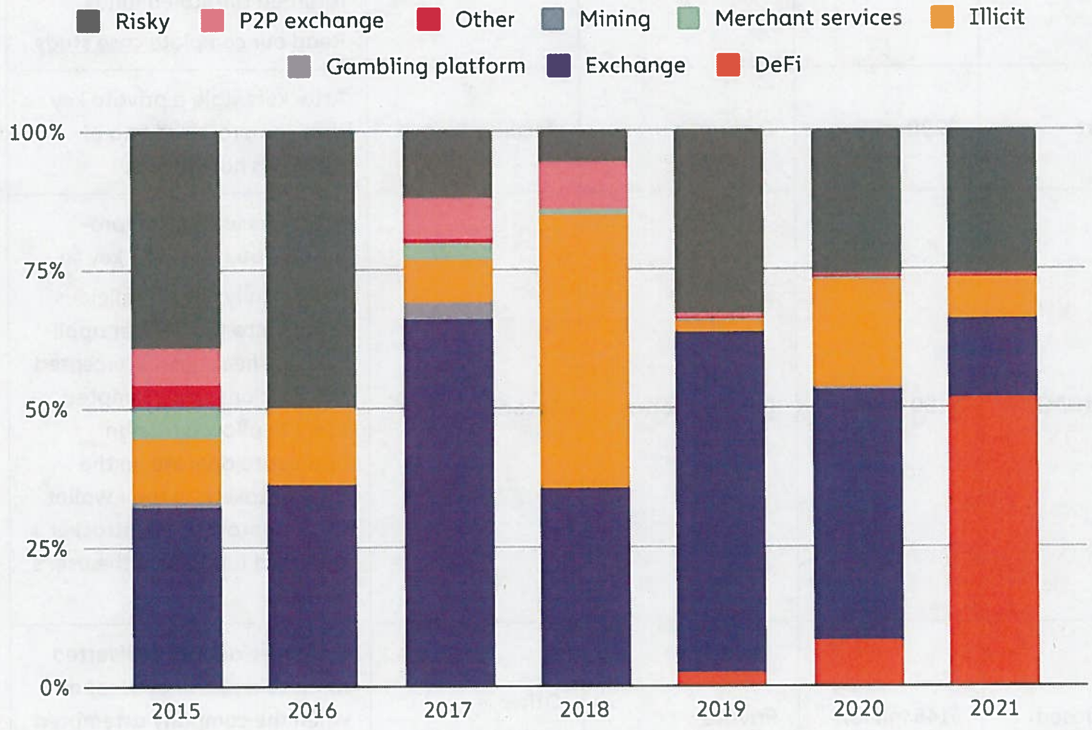


In 2020 and 2021, lending platforms such as yield farming protocols endured the largest losses, with $923 million in total stolen funds and 64 theft incidents. Infrastructure services like cross-chain protocols and oracles-as-a-service came in close second, with DEXes and DAOs reckoning with significant thefts as well.

Following the money: the final destinations of stolen cryptocurrencies

In the aftermath of cryptocurrency thefts, more stolen funds flowed to DeFi platforms (51%) and risky services (25%) this year than ever before. Centralized exchanges, once a top destination for stolen funds, fell out of favor in 2021, receiving less than 15% of the funds. This is likely due to the embrace of AML and KYC procedures among major exchanges—an existential threat to the anonymity of cybercriminals.

Destination of stolen funds | 2015–2021



Note: "Risky" refers to services like mixers, high-risk exchanges, and services based in high-risk jurisdictions.

The biggest cryptocurrency thefts of 2021

As is the case most years, the ten largest hacks of 2021 accounted for a majority of the funds stolen at $1.81 billion. Seven of these ten attacks targeted DeFi platforms in particular. The table below breaks down the details of each theft.

The 10 Largest Cryptocurrency Thefts of 2021

Victim	Amount stolen (USD)	Service Type	Hack Type	Description
Poly Network	$613 million	DeFi platform	Code exploit	An attacker exploited cross-chain relay contracts to extract Poly Network funds from three different chains: Ethereum, BSC, and Polygon. The attacker ultimately returned the stolen funds. Read our complete case study.
BitMart	$200 million	Exchange	Security Breach	Attackers stole a private key that compromised two of BitMart's hot wallets.
BadgerDAO	$150 million	DeFi platform	Security Breach	Attackers used a compromised cloudflare API key to periodically inject malicious scripts into the Badger application. The scripts intercepted transactions and prompted users to allow a foreign address to operate on the ERC-20 tokens in their wallet. Once approved, the attacker siphoned funds from the user's wallets.
Undisclosed	$145 million	Private	Other — Embezzlement	Employee allegedly diverted funds to a personal account when the company attempted to transfer funds between financial accounts.

Continued on the next page

Venus	$145 million	DeFi platform	Code Exploit	Attackers manipulated the price of XVS, Venus Protocol's governance token, in order to borrow quantities of BTC and ETH in excess of XVS's actual value. When the governance token's price declined and the collateral of the users who defaulted on their loans was liquidated, Venus was left with a debt of $145 million.
BXH	$139 million	DeFi platform	Other — Leaked Private Keys	An unidentified member of BXH's technical team allegedly leaked an administrator's private key.
Cream Finance	$130 million	DeFi platform	Flash Loan	First, attackers initiated a series of flash loans to mint -$1.5M of crYUSD. Then, the attacker took advantage of Cream's PriceOracleProxy function to artificially inflate the value of its crYUSD to ~$3B. $2B of this was withdrawn in order to repay the attacker's outstanding flash loans, while the remaining $1B was used to drain all of Cream's assets available for lending ($130M).
Vulcan Forged	$103 million	DeFi platform	Security Breach	Attacker gained access to the private keys of 96 addresses and sent their contents to hacker-controlled wallets.
Undisclosed	$91 million	DeFi platform	Code Exploit	Attacker used the platform's content delivery network (CDN) to respond to queries with malicious code that stole user assets
Undisclosed	$91 million	Exchange	Security Breach	Attacker gained access to the private keys of the service's internet-connected hot wallets.

2021 in cryptocurrency theft: A cautionary tale for DeFi developers

As the total value locked in DeFi climbs to ever-greater all-time highs—$256 billion at last peak—so too does the risk of exploitation. If there's one takeaway from the meteoric rise of thefts from DeFi platforms, it's the need for smart contract security and price oracle accuracy. Code audits, decentralized oracle providers, and an altogether more rigorous approach to platform security could be the ideal means to that end.

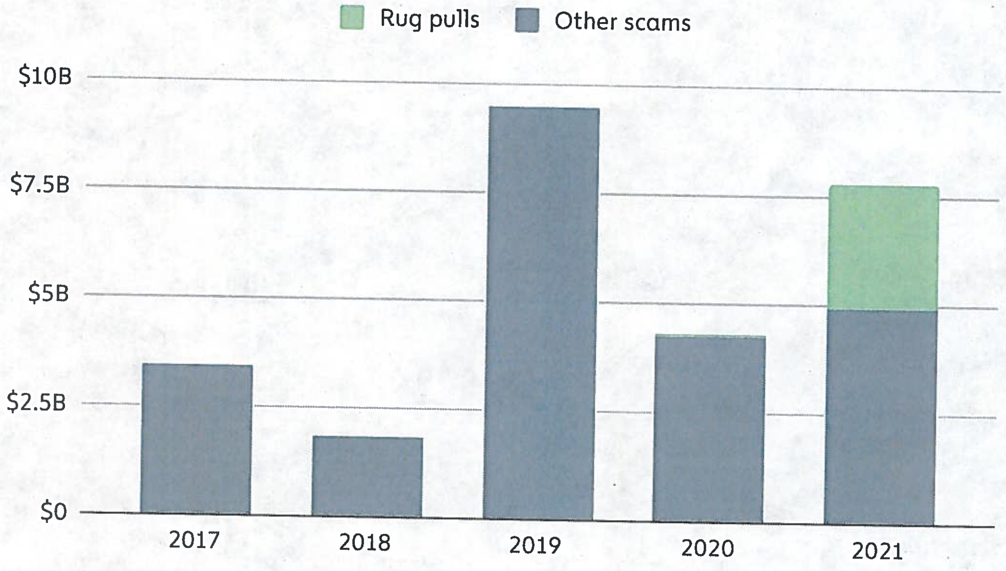
Fortunately, even when these functions do fail and cryptocurrencies are stolen, blockchain analysis can help. Investigators with a full picture of the movement of funds from address to address can take advantage of opportunities to halt assets in transit, stopping bad actors before they cash out.

Scams

The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Scam Revenue Close to All-time Highs

Scams were once again the largest form of cryptocurrency-based crime by transaction volume, with over $7.7 billion worth of cryptocurrency taken from victims worldwide.

Total yearly cryptocurrency value received by scammers | 2017–2021



That represents a rise of 81% compared to 2020, a year in which scamming activity dropped significantly compared to 2019, in large part due to the absence of any large-scale Ponzi schemes. That changed in 2021 with Finiko, a Ponzi scheme primarily targeting Russian speakers throughout Eastern Europe, netting more than $1.1 billion from victims.

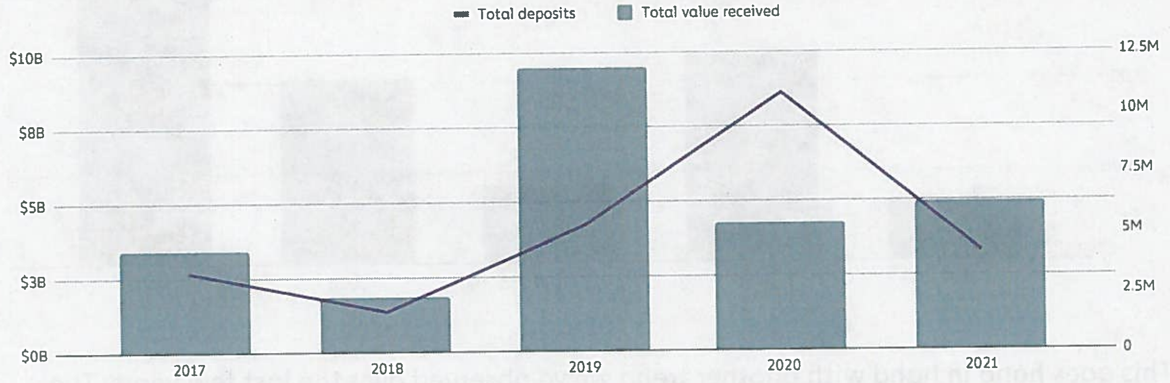
Another change that contributed to 2021's increase in scam revenue: the emergence of rug pulls, a relatively new scam type particularly common in the DeFi ecosystem, in which the developers of a cryptocurrency project — typically a new token — abandon it unexpectedly, taking users' funds with them. We'll look at both rug pulls and the Finiko Ponzi scheme in more detail later in the report.

As the largest form of cryptocurrency-based crime and one uniquely targeted toward new users, scamming poses one of the biggest threats to cryptocurrency's continued adoption. But as we'll explore, some cryptocurrency businesses are taking innovative steps to leverage blockchain data to protect their users and nip scams in the bud before potential victims make deposits.

Investment scams in 2021: More scams, shorter lifespans

While total scam revenue increased significantly in 2021, it stayed flat if we remove rug pulls and limit our analysis to financial scams — even with the emergence of Finiko. At the same time though, the number of deposits to scam addresses fell from just under 10.7 million to 4.1 million, which we can assume means there were fewer individual scam victims.

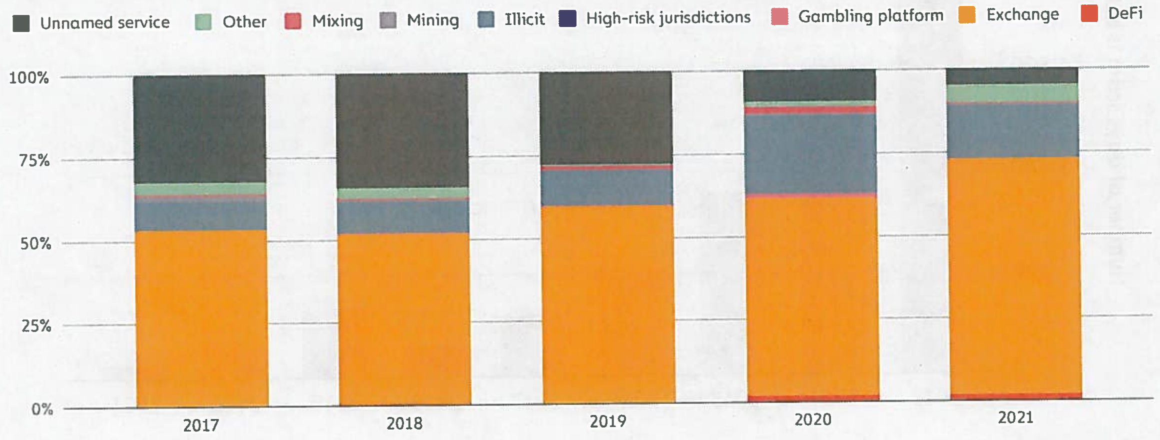
Total yearly cryptocurrency value received by investment scams | 2017–2021



This also tells us that the average amount taken from each victim increased.

Scammers' money laundering strategies haven't changed all that much. As was the case in previous years, most cryptocurrency sent from scam wallets ended up at mainstream exchanges.

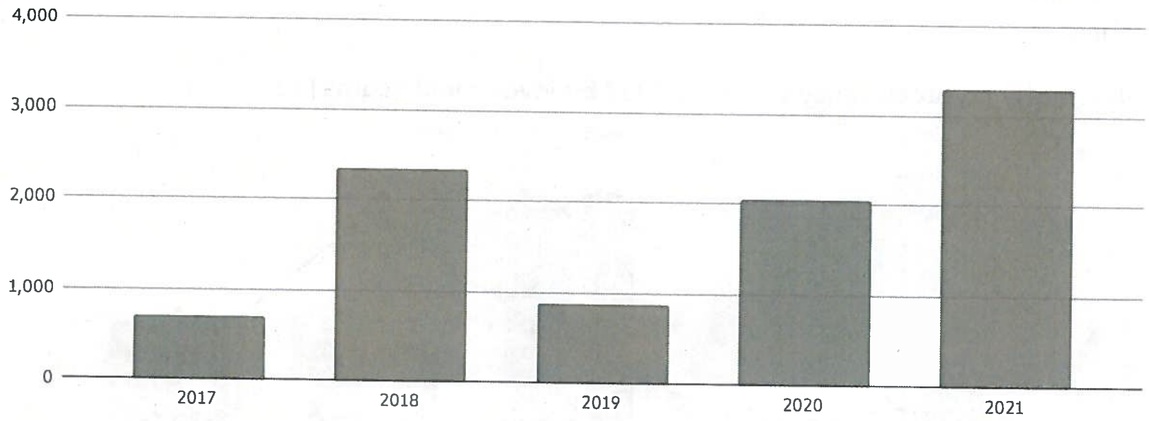
Destination of funds leaving investment scam addresses by year | 2017–2021



Exchanges using Chainalysis KYT for transaction monitoring can see this activity in real time, and take action to prevent scammers from cashing out.

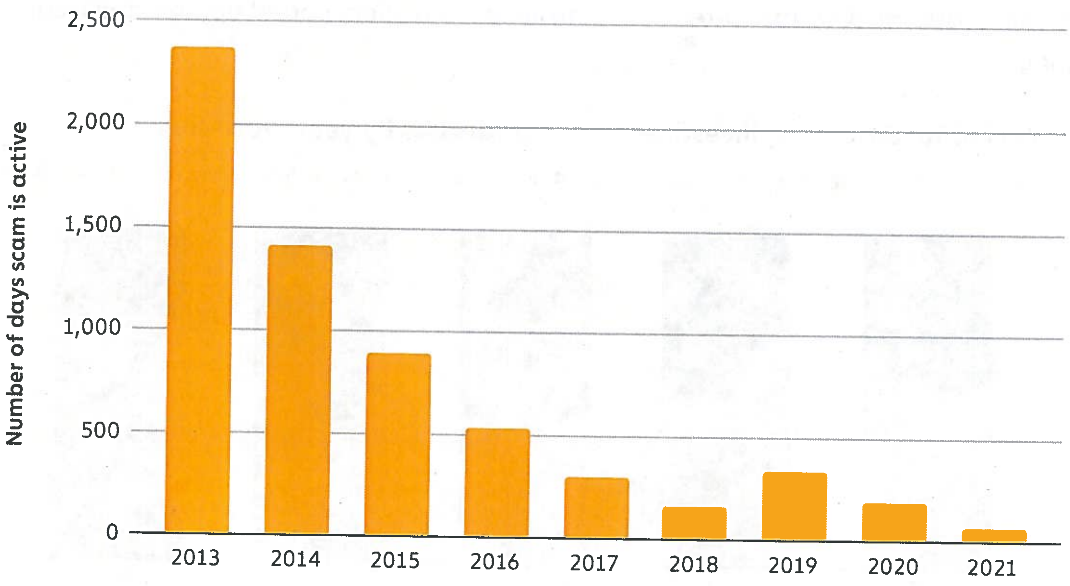
The number of financial scams active at any point in the year — active meaning their addresses were receiving funds — also rose significantly in 2021, from 2,052 in 2020 to 3,300.

Total number of unique active investment scams by year | 2017–2021



This goes hand in hand with another trend we've observed over the last few years: The average lifespan of a financial scam is getting shorter and shorter.

Lifespan of average scam by year | 2013–2021



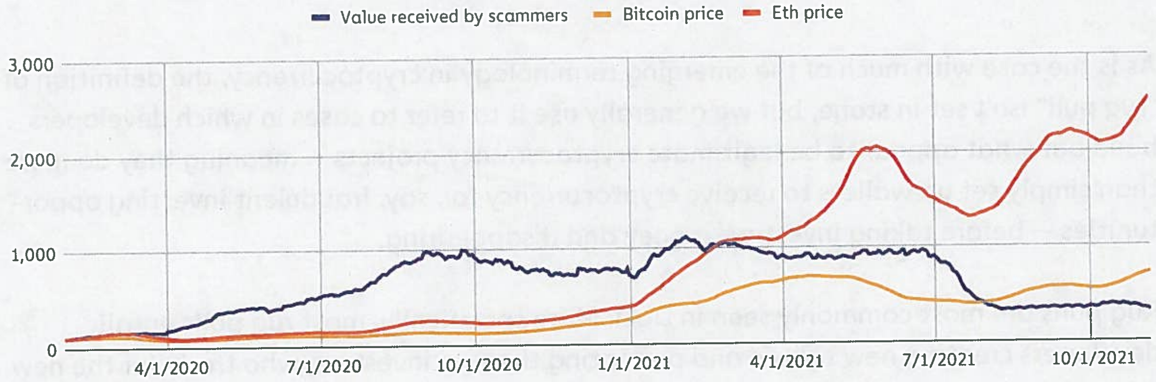
The average financial scam was active for just 70 days in 2021, down from 192 in 2020. Looking back further, the average cryptocurrency scam was active for 2,369 days, and the figure has trended steadily downwards since then. One reason for this could be that investigators are getting better at investigating and prosecuting scams. For instance, in

September 2021, the CFTC filed charges against 14 investment scams touting themselves as providing compliant cryptocurrency derivative trading services — a common scam typology in the space — whereas in reality they had failed to register with the CFTC as futures commission merchants. Previously, these scams may have been able to continue operating for longer. As scammers become aware of these actions, they may feel more pressure to close up shop before drawing the attention of regulators and law enforcement.

At the same time, we're seeing the end of a long-standing statistical relationship between cryptocurrency asset prices and scamming activity. Scams typically come in waves corresponding with sustained price growth in popular cryptocurrencies like Bitcoin and Ethereum, which typically also lead to influxes of new users. We see this reflected in the chart below — scamming activity spiked following bull runs in 2017 and 2020.

This isn't all that surprising. New, less savvy users attracted by cryptocurrency's growth are more likely to fall for scams than more seasoned users. However, the relationship between asset prices and scamming activity now appears to be disappearing.

Index: Total value received by scams vs. ETH and BTC price, 30-day moving average
Index: Jan 2020 = 100 | JAN 2020– NOV 2021

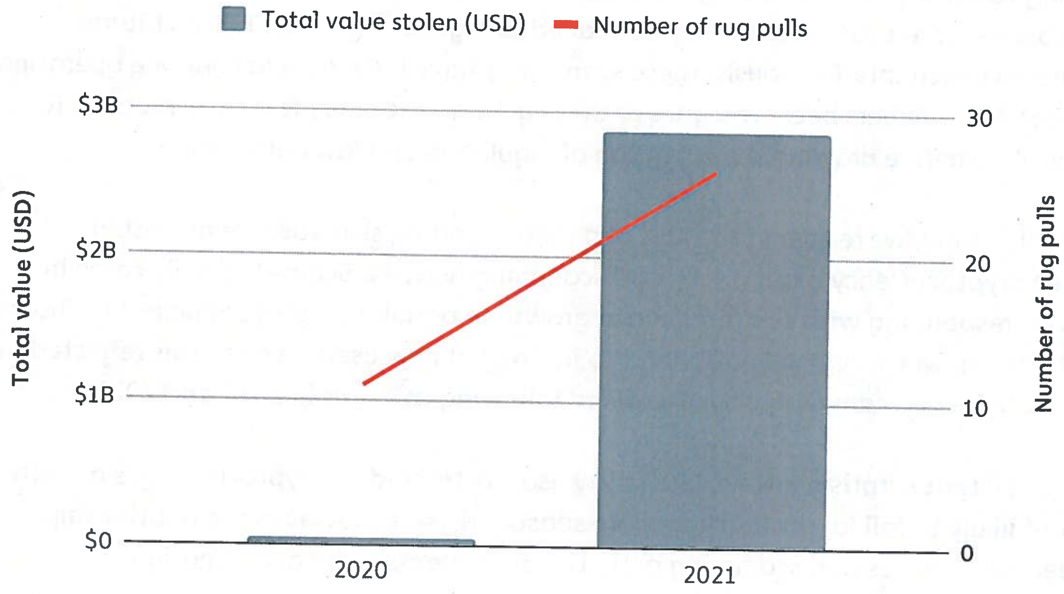


Above, we see scam activity rise in concert with Bitcoin and Ethereum prices until 2021, when scamming activity stays flat and even begins to drop regardless of whether prices rise or fall.

Rug pulls are the latest innovation in scamming

Rug pulls have emerged as the go-to scam of the DeFi ecosystem, accounting for 37% of all cryptocurrency scam revenue in 2021, versus just 1% in 2020.

Total cryptocurrency value stolen in rug pulls versus number of rug pulls | 2020 VS. 2021



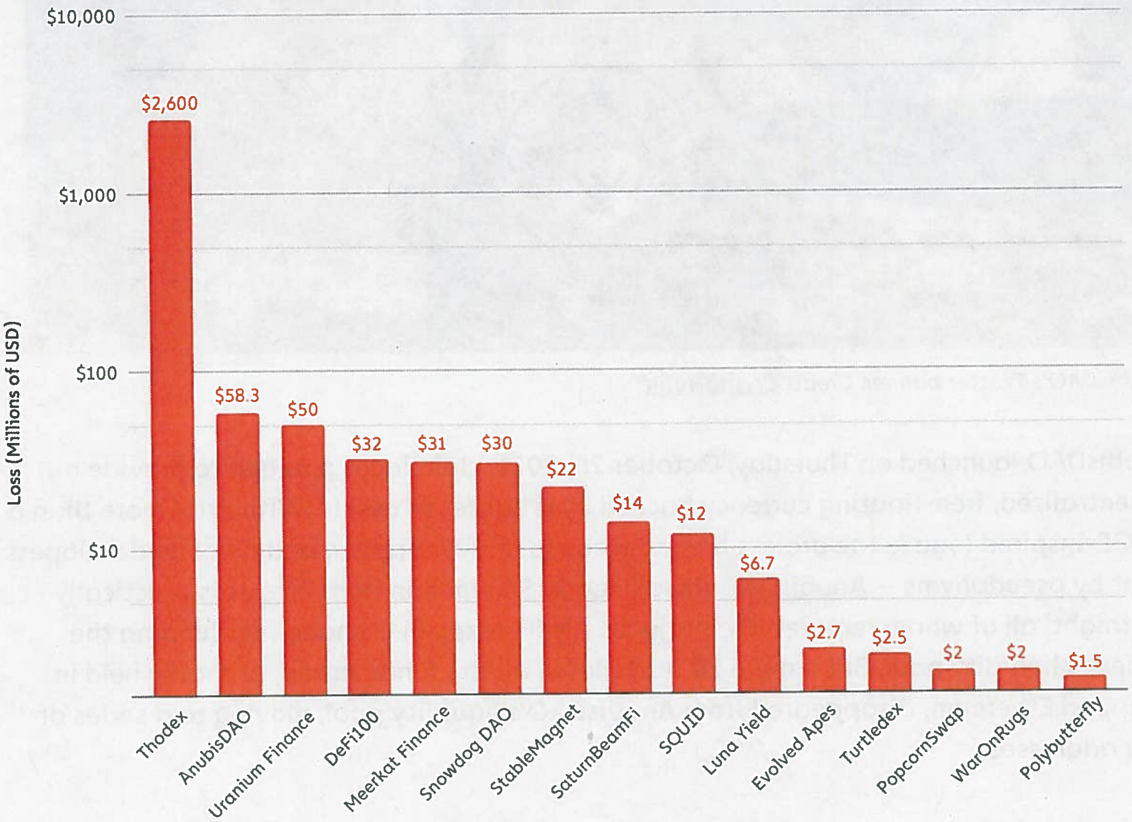
All in all, rug pulls took in more than $2.8 billion worth of cryptocurrency from victims in 2021.

As is the case with much of the emerging terminology in cryptocurrency, the definition of "rug pull" isn't set in stone, but we generally use it to refer to cases in which developers build out what appear to be legitimate cryptocurrency projects — meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investing opportunities — before taking investors' money and disappearing.

Rug pulls are most commonly seen in DeFi. More specifically, most rug pulls entail developers creating new tokens and promoting them to investors, who trade for the new token in the hopes the token will rise in value, which also provides liquidity to the project — that's how most DeFi projects start. In rug pulls, however, the developers eventually drain the funds from the liquidity pool, sending the token's value to zero, and disappear. Rug pulls are prevalent in DeFi because with the right technical know-how, it's cheap and easy to create new tokens on the Ethereum blockchain or others and get them listed on decentralized exchanges (DEXes) without a code audit. That last point is crucial — decentralized tokens are meant to be designed in such a way that investors holding governance tokens can vote on things like how assets in the liquidity pool are used, which would make it impossible for the developers to drain the pool's funds. While code audits that would catch these vulnerabilities are common in the space, they're not required in order to list on most DEXes, hence why we see so many rug pulls.

The chart below shows 2021's top 15 rug pulls in order of value stolen.

2021 Top 15 rug pulls by cryptocurrency value stolen | 2021

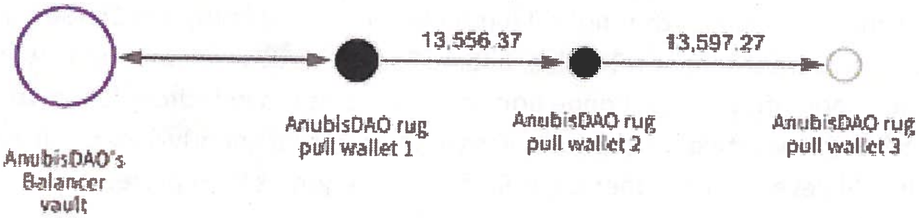


It's important to remember that not all rug pulls start as DeFi projects. In fact, the biggest rug pull of the year centered on Thodex, a large Turkish centralized exchange whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. In all, users lost over $2 billion worth of cryptocurrency, which represents nearly 90% of all value stolen in rug pulls. However, all the other rug pulls in 2021 began as DeFi projects.

AnubisDAO, the second-biggest rug pull of 2021 at over $58 million worth of cryptocurrency stolen, provides an excellent example of how rug pulls in DeFi work.

AnubisDAO's Twitter banner. Credit CryptoHubK

AnubisDAO launched on Thursday, October 28, 2021, claiming it planned to provide a decentralized, free-floating currency backed by a basket of assets. With little more than a DOGE-inspired logo — the project had no website or white paper, and all of its developers went by pseudonyms — AnubisDAO raised nearly $60 million from investors practically overnight, all of whom received the project's ANKH token in exchange for funding the project's liquidity pool. But a mere 20 hours later, all the funds raised, primarily held in wrapped Ethereum, disappeared from AnubisDAO's liquidity pool, moving to a series of new addresses.


13,556.37
13,597.27
AnubisDAO's Balancer vault
AnubisDAO rug pull wallet 1
AnubisDAO rug pull wallet 2
AnubisDAO rug pull wallet 3

We can see these transactions on the graph above. AnubisDAO used contracts created through Balancer's Liquidity Bootstrapping Protocol to receive and hold the wrapped Ethereum investors sent to their liquidity pool in exchange for ANKH tokens. However, the address that deployed the liquidity pool contract was already in possession of the vast majority of the liquidity provider (LP) tokens for that pool. 20 hours after the sale began, the address that created the pool cashed out it's massive holdings of LP tokens, allowing them to make off with nearly all the wrapped Ethereum and ANKH tokens in the pool. The thief then moved that wrapped Ethereum through a series of intermediary wallets. Soon after this, the Twitter account that had acted as the public face of AnubisDAO went offline, and ANKH's value plummeted to zero.

Since the theft, there's been a great deal of finger pointing and conflicting explanations. One of the project's pseudonymous founding developers claims another founder, who had access to AnubisDAO's liquidity pool, is solely responsible for the rug pull, while that founder claims to have fallen victim to a phishing attack that compromised the pool's private keys — the evidence that founder has supplied doesn't support that theory, however. At this time, all signs point to a standard rug pull, but it's unclear whether or not all of the developers were in on it.

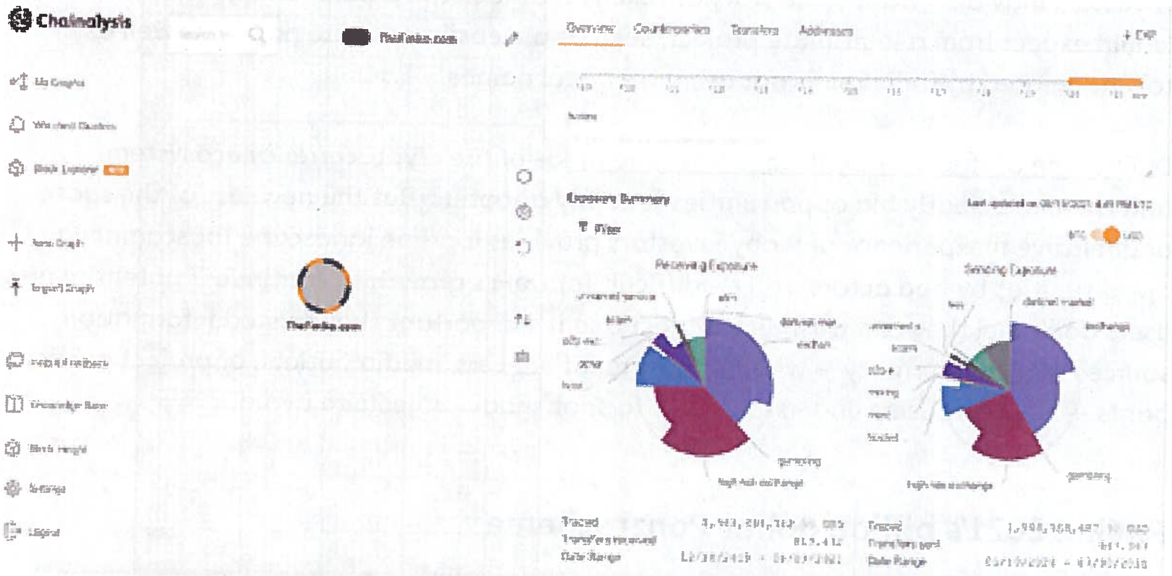
AnubisDAO should serve as a cautionary tale to investors evaluating similar opportunities. The most important takeaway is to avoid new tokens that haven't undergone a code audit. Code audits are a process by which a third-party firm analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are iron clad and contain no mechanisms that would allow for the developers to make off with investors' funds. They can also check for security vulnerabilities that could be exploited by hackers. OpenZeppelin is one example of a firm that provides code audits, but there are several others that are also considered trustworthy. Investors may also want to be wary of tokens that lack the public-facing materials one would expect from a legitimate project, such as a website or white paper, as well as tokens created by individuals not using their real names.

DeFi is one of the most exciting, innovative areas of the cryptocurrency ecosystem, and there are clearly big opportunities for early adopters. But the newness of the space and relative inexperience of many investors provides a prime landscape for scamming opportunities by bad actors. It'll be difficult for DeFi's growth to continue if potential new users don't feel they can trust new projects, so it's important that trusted information sources in cryptocurrency — whether they're influencers, media outlets, or project participants — help new users understand how to spot shady projects to avoid.

Finiko: 2021's billion dollar Ponzi scheme

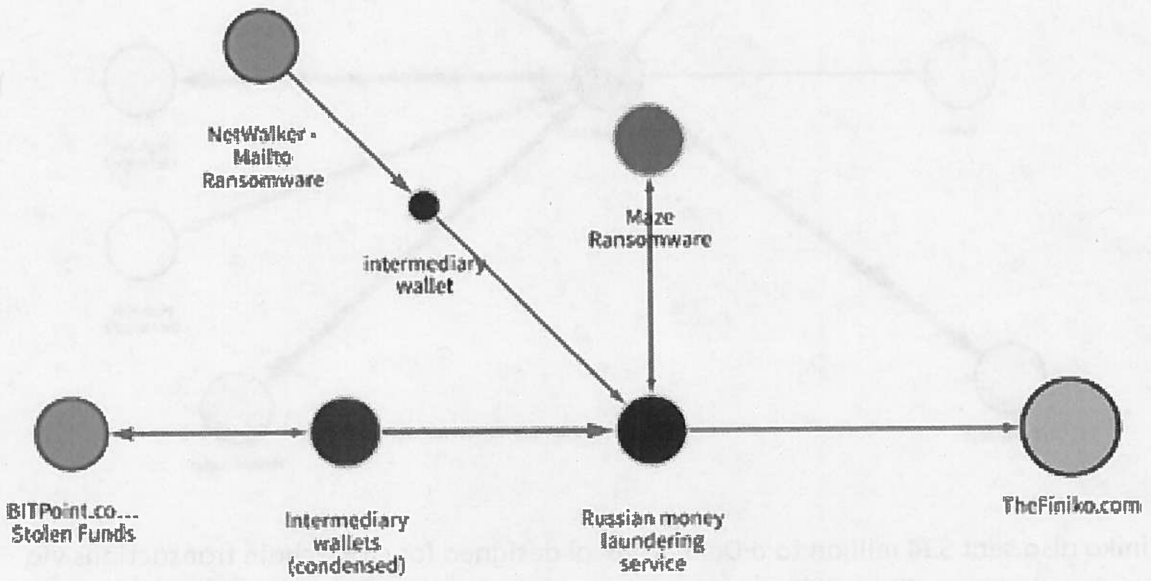
Finiko was a Russia-based Ponzi scheme that operated from December 2019 until July 2021, at which point it collapsed after users found they could no longer withdraw funds from their accounts with the company. Finiko invited users to invest with either Bitcoin or Tether, promising monthly returns of up to 30%, and eventually launched its own coin that traded on several exchanges.

According to the Moscow Times, Finiko was headed up by Kirill Doronin, a popular Instagram influencer who has been associated with other Ponzi schemes. The article notes that Finiko was able to take advantage of difficult economic conditions in Russia exacerbated by the Covid pandemic, attracting users desperate to make extra money. Chainalysis Reactor shows us how prolific the scam was.



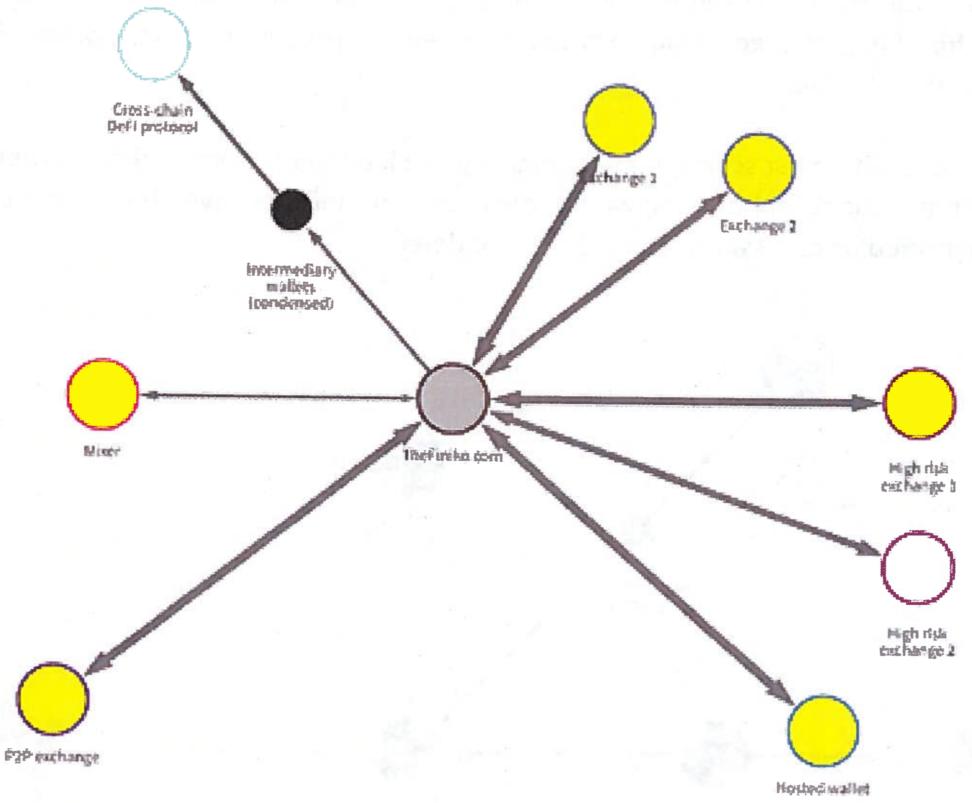
During the roughly 19 months it remained active, Finiko received over $1.5 billion worth of Bitcoin in over 800,000 separate deposits. While it's unclear how many individual victims were responsible for those deposits or how much of that $1.5 billion was paid out to investors to keep the Ponzi scheme going, it's clear that Finiko represents a massive fraud perpetrated against Eastern European cryptocurrency users, predominantly in Russia and Ukraine.

As is the case with most scams, Finiko primarily received funds from victims' addresses at mainstream exchanges. However, we can also see that Finiko received funds from what we've identified as a Russia-based money launderer.

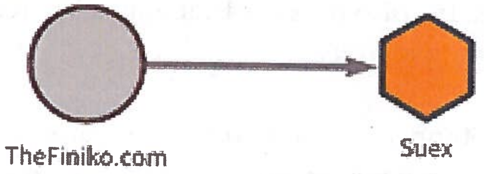

NetWalker - Mailto Ransomware
intermediary wallet
Maze Ransomware
BITPoint.co... Stolen Funds
Intermediary wallets (condensed)
Russian money laundering service
TheFiniko.com

This launderer has received millions of dollars' worth of cryptocurrency from addresses associated with ransomware, exchange hacks, and other forms of cryptocurrency-based crime. While the amount the service has sent to Finiko is quite small — under 1 BTC total — it serves as an example of how a scam can also be used to launder funds derived from other criminal schemes. It's also possible that Finiko has received funds from other laundering services we've yet to identify.

Finiko sent most of its more than $1.5 billion worth of cryptocurrency to mainstream exchanges, high-risk exchanges, a hosted wallet service, and a P2P exchange. However, we don't know what share of those transfers represent payments to victims in order to give the appearance of successful investments.



Finiko also sent $34 million to a DeFi protocol designed for cross-chain transactions via a series of intermediary wallets, where it was likely converted into ERC-20 tokens and sent elsewhere. It also sent roughly $3.9 million worth of cryptocurrency to a few popular mixing services. Most interesting of all perhaps is Finiko's transaction history with Suex, an OTC broker that was sanctioned by OFAC for its role in laundering funds associated with scams, ransomware attacks, and other forms of cryptocurrency-based crime.



Between March and July of 2020, Finiko sent over $9 million worth of Bitcoin to an address that now appears as an identifier on Suex's entry into the Specially Designated Nationals (SDN) List. This connection underlines the prolificness of Suex as a money laundering service, as well as the crucial role of such services generally in allowing large-scale cybercriminal operations like Finiko to victimize cryptocurrency users.

Soon after Finiko's collapse in July 2021, Russian authorities arrested Doronin, and later also nabbed Ilgiz Shakirov, one of his key partners in running the Ponzi scheme. Both men remain in custody, and arrest warrants have reportedly been issued for the rest of Finiko's founding team.

How one cryptocurrency platform is saving users from scams

Mainstream cryptocurrency platforms like exchanges are in the perfect position to fight back against scams and instill more trust in cryptocurrency by warning users or even preventing them from executing those transactions. One popular platform did just that in 2021, and the results were extremely promising.

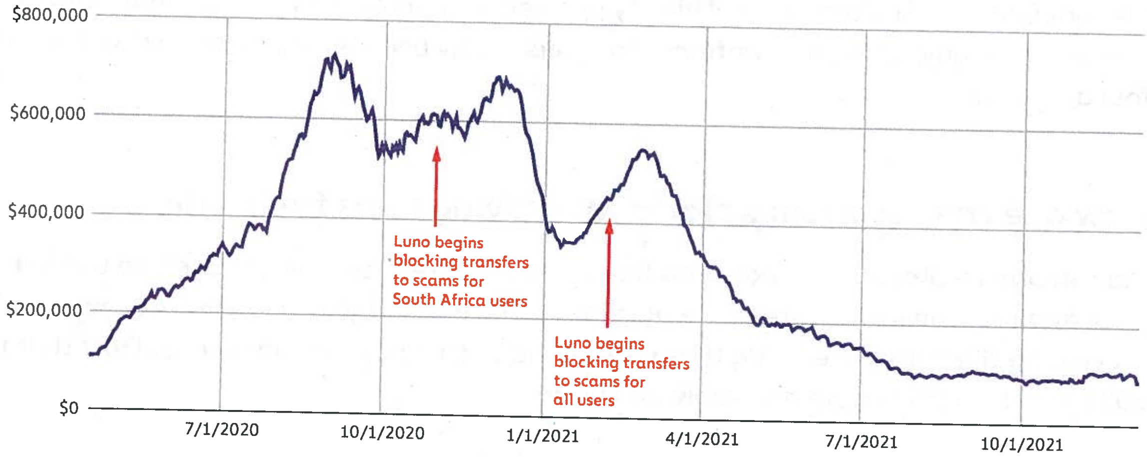
Luno is a leading cryptocurrency platform operating in over 40 countries, with an especially heavy presence in South Africa. In 2020, a major scam was targeting South African cryptocurrency users, promising outlandishly large investment returns. Knowing that its users were at risk, Luno decided to take action in partnership with Chainalysis.

The first step was a warning and education campaign. Using in-app messages, help center articles, emails, webinars, social media posts, YouTube videos, and even one-on-one conversations, Luno showed users how to spot the red flags that indicate an investment opportunity is likely a scam, and taught them to avoid pitches that appear too good to be true.

Luno then went a step further and began preventing users from sending funds to addresses it knew belonged to scammers. That's where Chainalysis came in. As the leading blockchain data platform, we have an entire team dedicated to unearthing cryptocurrency scams and tagging their addresses in our compliance products. With that data, Luno was able to halt users' transfers to scams before they were processed. It was a drastic strategy in many ways — cryptocurrency has historically been built on an ethos of financial freedom, and some users were likely to chafe at a perceived limitation on their ability to transact. But thanks to Chainalysis' best in class cryptocurrency address attributions, Luno was able to establish the trust necessary to sell customers on the strategy.

Luno first began blocking scam payments for South African users only in November 2020, and then rolled the feature out worldwide in January 2021. The plan worked, and transfers from Luno wallets to scams fell drastically over the course of 2021.

Daily value received by scams from Luno, 30-day moving average



The moving 30-day average daily transaction volume of transfers to scams fell 88% from $730,000 at its peak in September 2020, to just $90,000 by November. One customer summed up the results perfectly, saying, "Thank you, Luno. I was about to lose my pension and savings."

Scams represent a huge barrier to successful cryptocurrency adoption, and fighting them can't be left only to law enforcement and regulators. Cryptocurrency businesses, financial institutions, and, of course, Chainalysis have an important role to play as well. With this strategy, Luno took a courageous step towards establishing greater trust and safety in cryptocurrency, which we hope to continue to see grow in the industry.

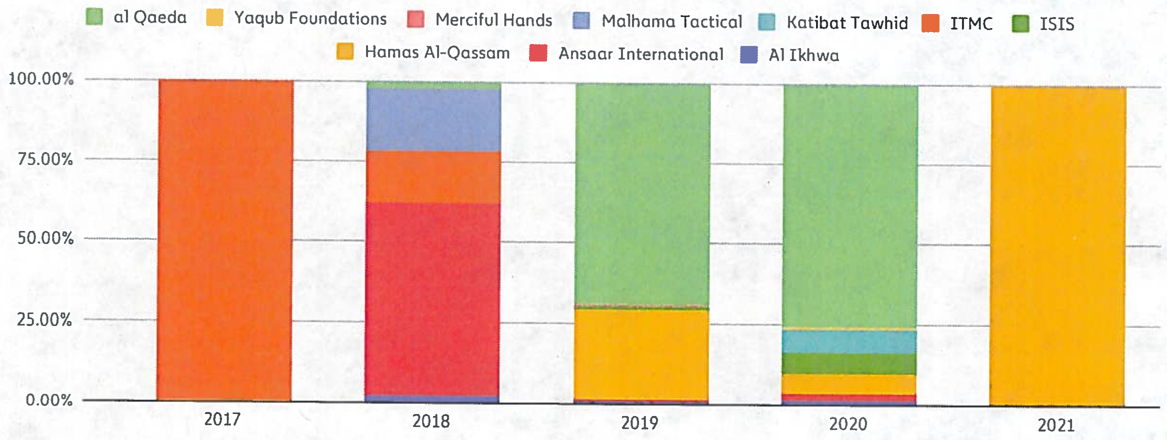
Terrorism Financing

Al-Qaeda, ISIS, and Hamas Among Terrorist Groups Fundraising in Cryptocurrency—With Government Seizures Close Behind

By the end of 2021, we've identified a number of terrorist organizations that have attempted to finance their operations with cryptocurrency. What's harder to find, however, is a group that has gotten away with it.

- In 2019 and 2020, al-Qaeda raised cryptocurrency through Telegram channels and Facebook groups. Thanks to the FBI, HSI, and IRS-CI, more than $1 million was seized from a money service business (MSB) operator who facilitated some of these transactions.
- In early Spring of 2021, al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations. In July, the Israeli government seized much of it from associated MSBs.

Share of total terrorism financing activity by organization | 2017–2021



In the following section, we isolate three cases from 2021—one in June, one in July, and another in December—that showcase governments' recent successes in the fight against cryptocurrency-financed terrorism.

Case 1: Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns

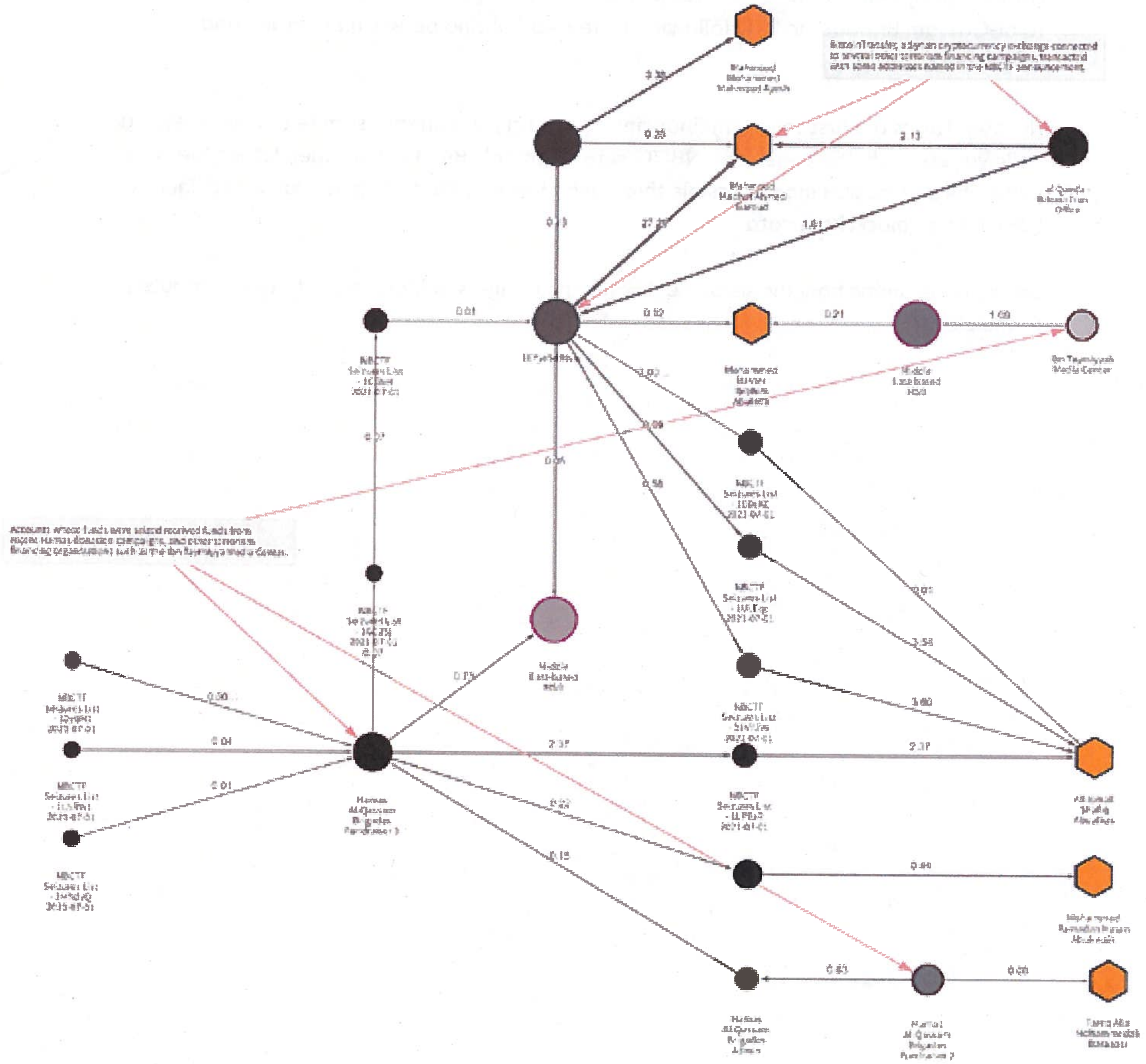
On June 30th, Israel's National Bureau for Counter Terror Financing (NBCTF) announced the seizure of cryptocurrency held by several wallets associated with donation campaigns carried out by Hamas. The action came after a sizable growth in cryptocurrency donations to al-Qassam Brigades in May following increased fighting between the group and Israeli forces.

Notably, this is the first terrorism financing-related cryptocurrency seizure to include such a wide variety of digital currencies. NBCTF seized not only Bitcoin, but Ether, Tether, XRP, and more. The seizure was made possible through an investigation of open-source intelligence (OSINT) and blockchain data.

Below, we examine how the second of these—the analysis of blockchain data—contributed to the case.

How funds moved from donation addresses to exchanges

The Chainalysis Reactor graph below shows the Bitcoin portion of the transactions carried out by many of the addresses listed in the NBCTF announcement. Many of these addresses have been attributed to individuals connected to the donation campaigns.


Based in Turkey, a Syrian cryptocurrency exchange connected to several other terrorism financing campaigns, transacted with some addresses named in the NBCTF announcement.

Accounts whose funds were seized received funds from Hamas donation campaigns, and other terrorist financing organizations such as the Ibn Taymiyya Media Center.

The orange hexagons represent deposit addresses hosted at large, mainstream cryptocurrency exchanges that are controlled by individuals named in the NBCTF announcement. As we can see, the funds often passed through intermediary wallets, high-risk cryptocurrency exchanges, and money services businesses (MSBs) before reaching the exchanges from which the named individuals likely hoped to cash out.

Interestingly, we can see that two donation addresses named in the announcement received funds from addresses associated with the Idlib office of BitcoinTransfer (top right of graph), a Syrian cryptocurrency exchange connected to previous terrorism financing cases. Another received funds from a Middle East-based MSB that had previously received funds from the Ibn Taymiyya Media Center (directly beneath the BitcoinTransfer cluster), an organization that has also been associated with terrorism financing in the past.

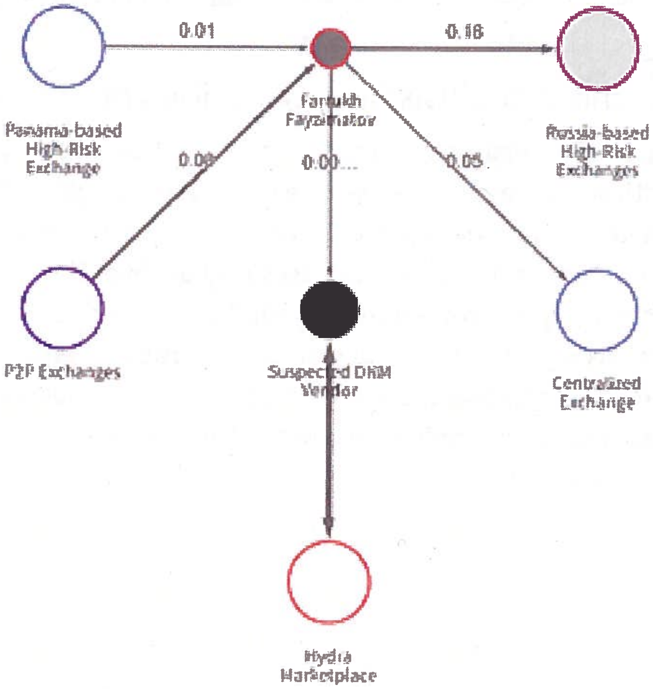
The value of blockchain analysis in conjunction with other data sources

This investigation is a perfect example of the value of blockchain analysis, especially when used in conjunction with other open source data. Israeli authorities analyzed OSINT to find Hamas' donation addresses and, with blockchain analysis tools, were able to follow the funds to find consolidation addresses and uncover the names of individuals associated with the campaigns. Up-to-date transaction data across several blockchains was crucial in this case as agents tracked and seized funds of several different cryptocurrencies, not just one. We applaud the Israeli authorities for a successful operation and look forward to providing valuable tools that facilitate more such successes for our government customers around the world.

Case 2: Terrorist Financier designated by the U.S. Office of Foreign Assets Control (OFAC)

On July 28, 2021, OFAC sanctioned Farrukh Furkatovitch Fayzimatov for having materially assisted and supported Hay'et Tahrir al-Sham (HTS), a militant group involved in the Syrian Civil War. Fayzimatov utilized social media to post propaganda, recruit new members, and solicit donations to purchase equipment for the benefit of HTS.

His fundraising efforts have been linked to an address tracked by Chainalysis, the details of which are depicted in the graph below.



On the left side of the graph, we find that Fayzimatov received funds directly from centralized and P2P exchanges that did not collect know-your-customer information. This indicates that the individuals sending bitcoin to Fayzimatov intended to keep their activity anonymous. On the right, we observe that Fayzimatov sent funds to high-risk exchanges based in Russia, one centralized exchange that did collect KYC information, and a small sum to a suspected vendor at Hydra Marketplace, a Russian darknet market.

Following the OFAC designation, Fayzimatov's on-chain activity ceased.

Case 3: Wales-based convicted terrorist caught using darknet market 'Bypass Shop'

In December, a 29-year-old man was sentenced to 16 months in jail for Bitcoin transactions made on the Bypass Shop, a darknet market for stolen credit card information.

The transactions were made from the man's wallet at an exchange, which prompted the company to issue a suspicious activity report. From there, police identified the man as Khuram Iqbal of Cardiff, and arranged for his arrest.

This was not Iqbal's first run-in with the law. Iqbal had been jailed in 2014 for possessing terrorist information and disseminating terrorist publications under the pseudonym Abu Irhaab—Arabic for "father of terrorism." In total, Iqbal possessed nine copies of the al-Qaeda magazine "Inspire," and published more than 800 links to extremist material on Facebook.

Before then, Iqbal made two attempts to join the jihadi cause by flying to Kenya and Turkey. He was deported on both occasions.

Blockchain analysis: Governments' best tool in the fight against cryptocurrency-financed terrorism

As terrorist organizations adopt further blockchain technologies and cryptocurrency fundraising techniques, it's critical for governments to keep up. Our 2021 findings indicate that many agencies have, and the rewards have been considerable.

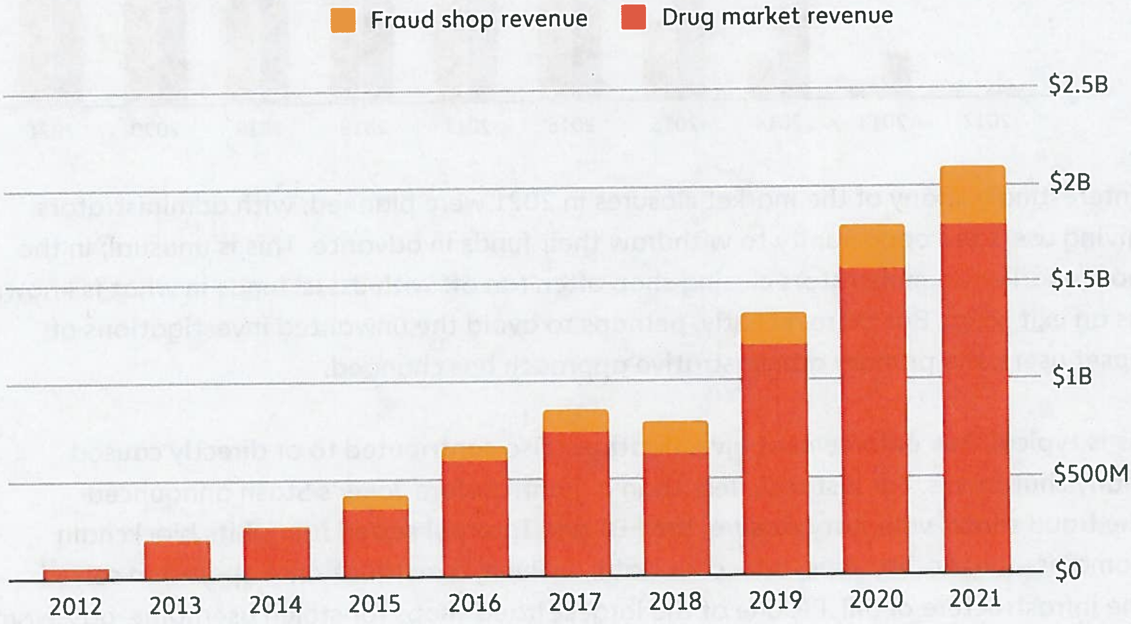
Governments that have embraced blockchain analysis have seized millions of dollars in cryptocurrency and stopped a number of terrorist financiers—further evidence that with the proper tools, investigators can cut terrorist organizations off from the funds that enable their rise.

Darknet Markets

Darknet Markets Hit All-time High in Revenue, Eclipsing $2 Billion, Despite Their Decline in Overall Number

Darknet markets set a new revenue record in 2021, bringing in a total of $2.1 billion in cryptocurrency. Roughly $300 million of this total was generated by fraud shops, which brokered the sale of stolen logins, credit cards, exploit kits, and more. The rest—more than $1.8 billion—was generated by drug-focused markets.

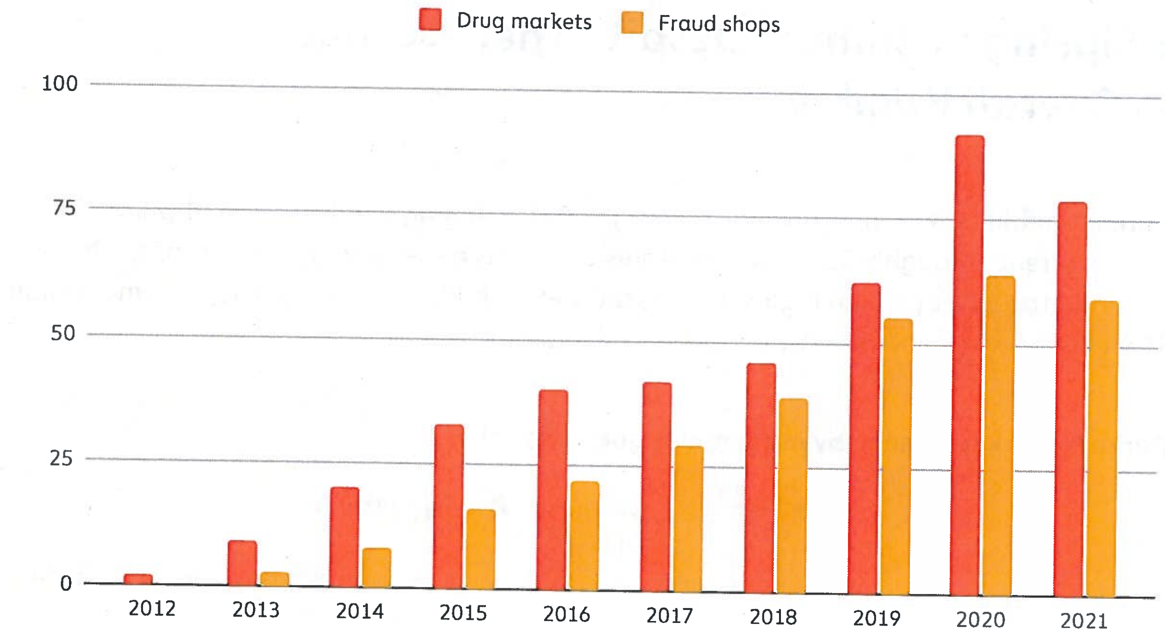
Darknet market revenue by market category | 2012-2021



We also identified an additional $112 million (not included above) in revenues for these categories from direct buyer-to-vendor sales, meaning sales that didn't use a darknet market as an intermediary. We discuss this trend in greater detail later in this section.

Despite this illicit industry's continued revenue growth, the number of active markets actually fell this year. By the end of 2021, there were five fewer fraud shops and 13 fewer drug-focused markets than at the end of 2020.

Number of active drug markets and fraud shops | 2012-2021



Interestingly, many of the market closures in 2021 were planned, with administrators giving users the opportunity to withdraw their funds in advance. This is unusual; in the past, market administrators closing shop often ran off with users' funds in what is known as an exit scam. But more recently, perhaps to avoid the unwanted investigations of upset users, the primary administrative approach has changed.

As is typical, law enforcement investigations also contributed to or directly caused many shutdowns. For instance, less than a month before Joker's Stash announced the fraud shop's voluntary closure, the FBI and Interpol seized four of its blockchain domains—.bazar, .lib, .emc, and .coin. Later, in June, a multinational operation seized the infrastructure of Slil_PP, one of the largest fraud shops for stolen username-password combinations. And in October, the Department of Justice announced the results of Dark HunTor, an operation that resulted in the arrest of 150 drug traffickers and the closure of two drug markets. Still other darknet markets, such as DarkMarket, Monopoly, and CanadianHeadquarters, have shuttered after being caught in similar precarious situations this year.

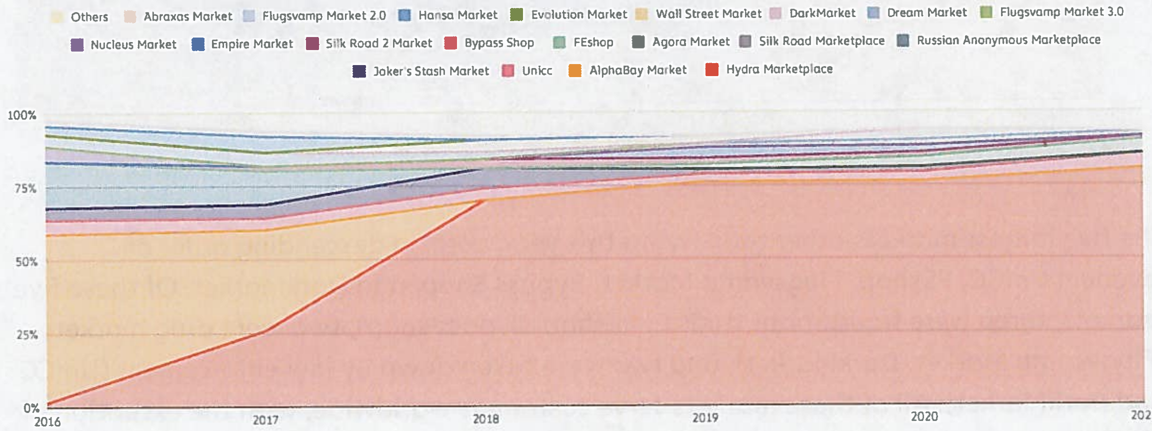
For the darknet markets that remain, competition is fiercer than ever, and competitors aren't afraid to play dirty. Data leaks, DDoS attacks, and doxxes are common occurrences in the space, according to Flashpoint's Senior Director of Research Ian Gray. For example, shortly after the relaunch of AlphaBay in August 2021, a DDoS attack was allegedly conducted on the marketplace by "mr_white," the administrator of the since-shuttered White House Market. Another DDoS attack, this one unattributed, took Cannazon, a marijuana-focused market, permanently offline. A third action, an alleged dox of Hydra market's administrators, was published on the hydra[.]expert domain in February.

These competitive threats, alongside other barriers to entry like finding a hosting provider and retaining vendors, have made opening and operating a darknet market too difficult for many would-be administrators—another explanation for the decline.

The Russia-based Hydra Market continues to dominate by total revenue, but other markets outside of Eastern Europe also thrive

Hydra, a market that serves only Russian-speaking countries, remains the largest darknet market by far. In 2021, Hydra accounted for 80% of darknet market revenue worldwide.

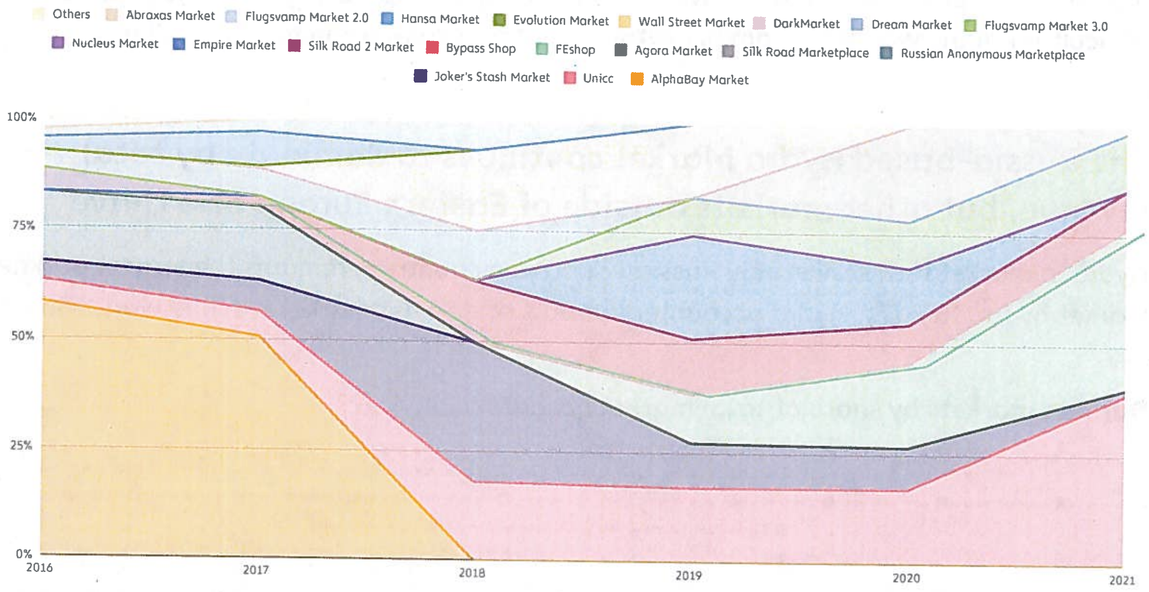
Darknet markets by share of total market | 2016-2021



Hydra is distinct for its size, Russian focus, and variety of offerings: users of Hydra can purchase both drugs and fraud-related goods and services on the website, though drugs account for the majority of its sales. However, Hydra is so large that it can prevent our data visualizations from showing the important role of other, more global markets.

Below, we exclude Hydra activity and find that the remaining markets are in much closer competition.

Darknet markets by share of total market (excluding Hydra) | 2016-2021

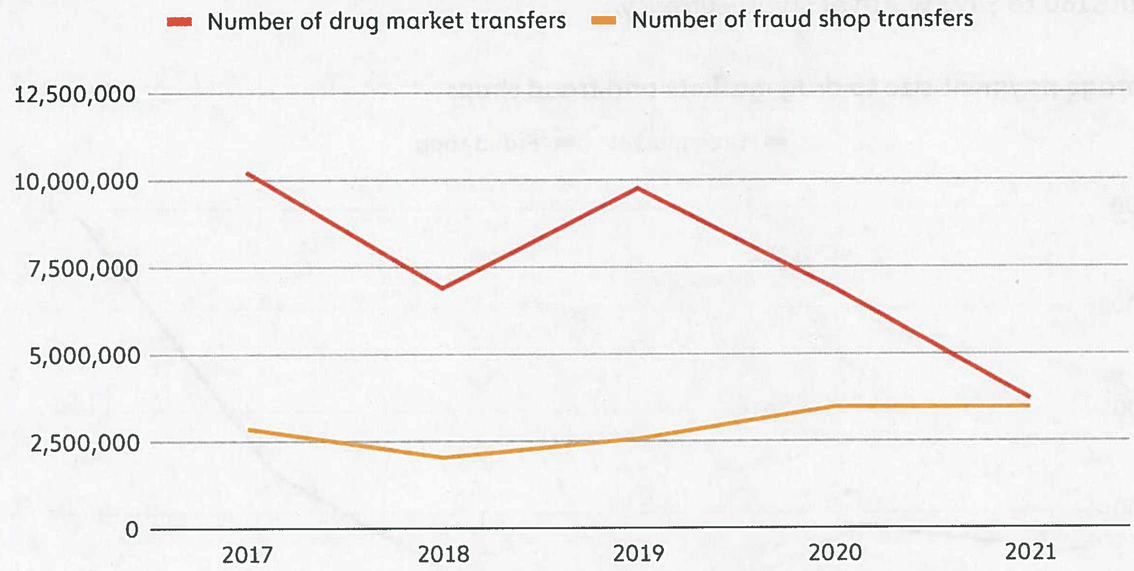


The five largest markets other than Hydra this year were, in descending order of revenue: UniCC, FEshop, Flugsvamp Market, Bypass Shop, and DarkMarket. Of these five markets, three were fraud shops (UniCC, FEshop, Bypass shop), two were drug markets (Flugsvamp Market, DarkMarket), and two were taken down by law enforcement (UniCC and DarkMarket). All of these markets serve customers worldwide, with the exception of Flugsvamp, which serves only Swedish users.

As the number of transfers to drug markets and their user counts dwindle, growing payment sizes more than compensate

Curiously, the number of transfers to drug-focused markets has fallen considerably over the past five years, from 11.7 million in 2016 to just 3.7 million this year.

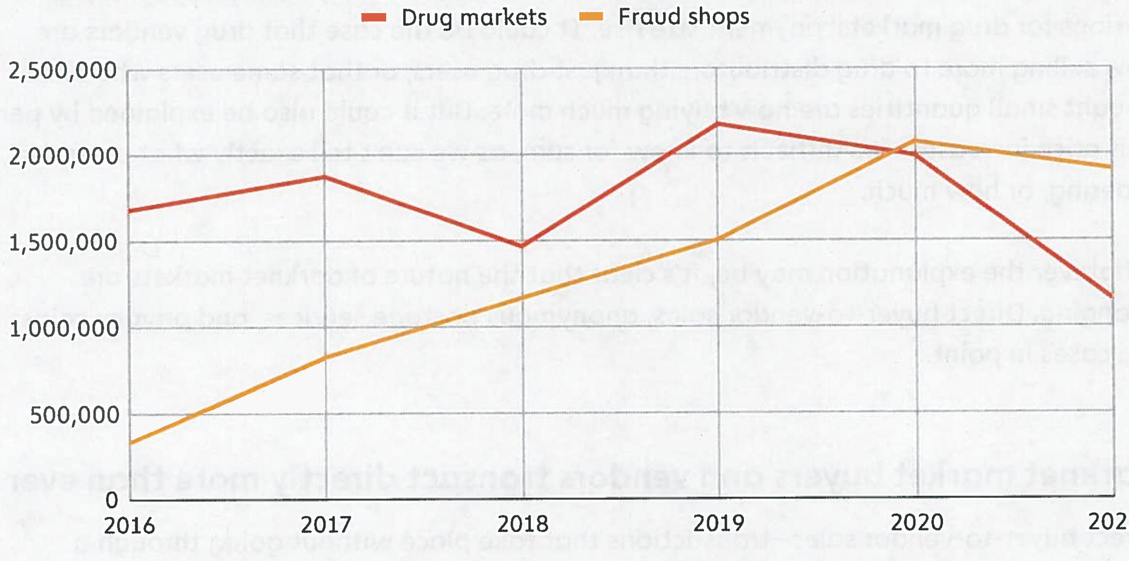
Number of transfers to drug markets and fraud shops | 2016-2021



An "active user" is defined as any wallet that has sent or received more than $5 worth of cryptocurrency to/from darknet markets during the year

The number of active users on drug markets has also undergone a decline, shrinking from almost 1.7 million in 2016 to 1.2 million in 2021.

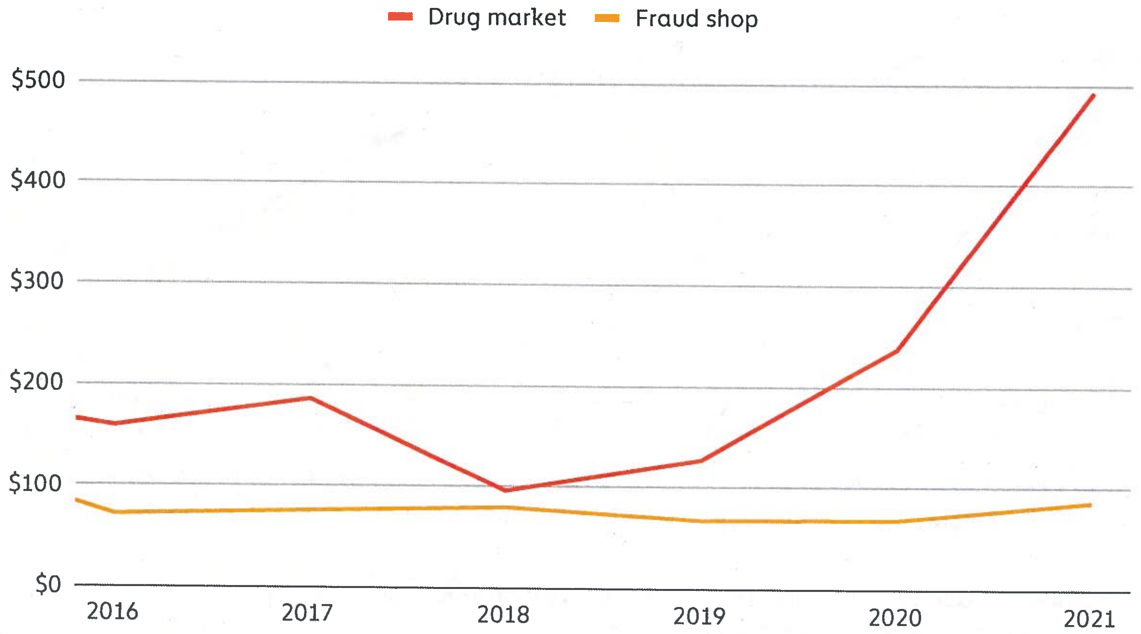
Number of active users of drug markets and fraud shops | 2016-2021



With drug market declines like these, one would expect overall drug market revenues to fall, but in fact they've done the opposite. From 2016 to 2021, drug market revenue growth averaged 35.7 percent per year. So if more users and more transfers aren't behind this growth, what is?

Our finding: bigger payments. From 2016 to 2021, the average payment size has leapt from $160 to $493 worth of cryptocurrency.

Average payment size to drug markets and fraud shops



Interestingly, this trend has only played out with drug-focused markets, as the average purchase price for fraud shops has remained flat. But there are several possible explanations for drug markets' payment size rise. It could be the case that drug vendors are now selling more to drug distributors than just drug users, or that some users who once bought small quantities are now buying much more. But it could also be explained by per unit price increases—it's difficult to know for sure, as we can't tell exactly what users are ordering, or how much.

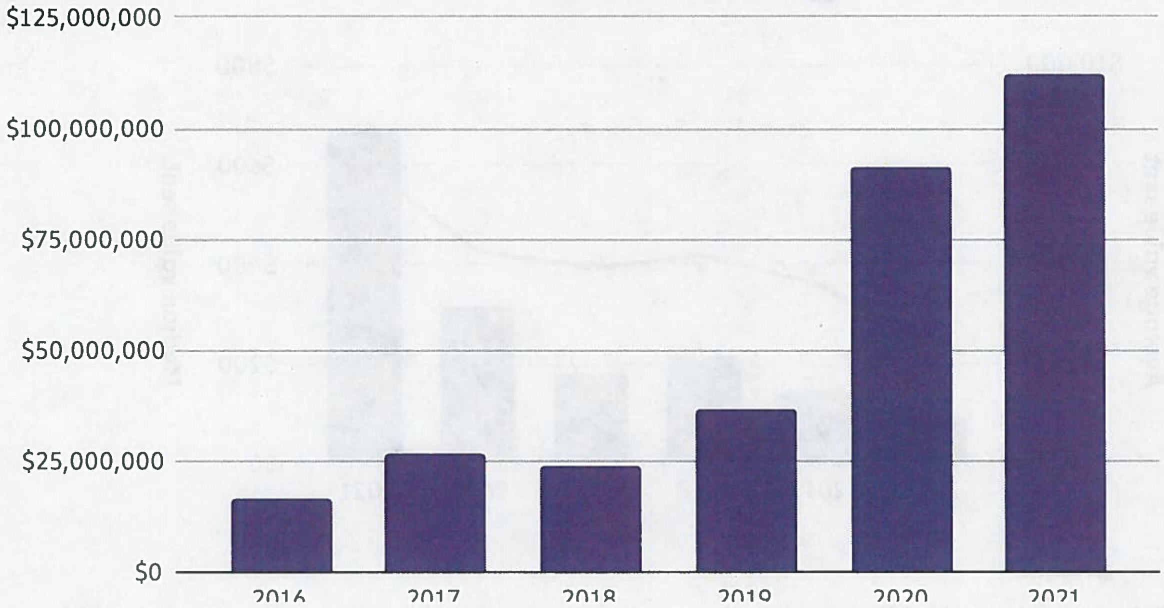
Whatever the explanation may be, it's clear that the nature of darknet markets are changing. Direct buyer-to-vendor sales, anonymous postage services, and privacy coins are cases in point.

Darknet market buyers and vendors transact directly more than ever

Direct buyer-to-vendor sales—transactions that take place without going through a darknet market—have been on the rise since 2019. We suspect that many of these buyer-vendor relationships were initially established on darknet markets, but that after a series of successful purchases, the buyers and vendors then arranged to transact off-market going forward.

Sales of this kind reached $112 million this year, equivalent to approximately 5% of total darknet market revenues.

Total value sent directly from darknet market buyers to vendors | 2016-2021



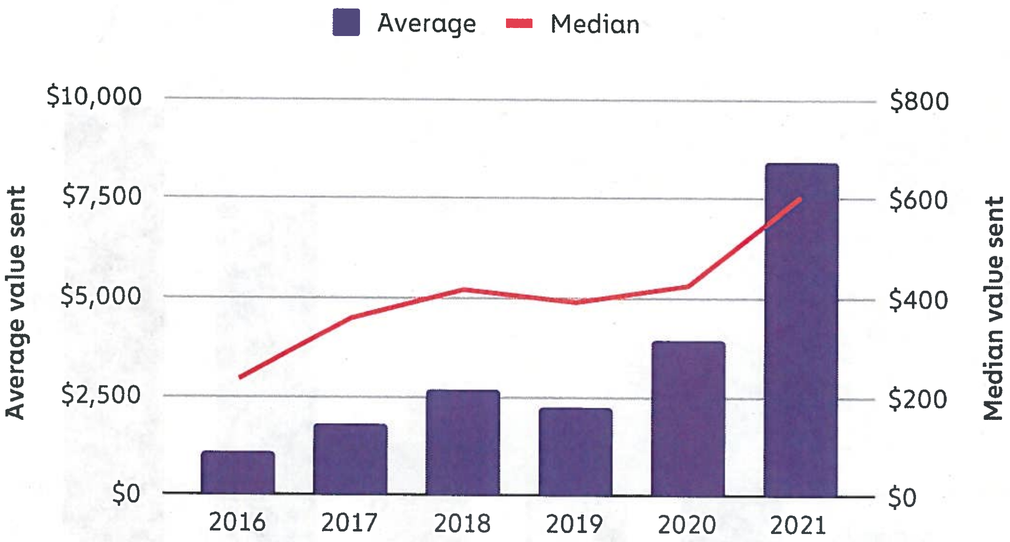
A user is considered a vendor if they have received more than $5,000 in cryptocurrency from darknet markets (DNMs) and are a net receiver of funds from DNMs. A user is considered a buyer if they have sent more than $100 in cryptocurrency to darknet markets and are a net sender of funds to DNMs.

This growth in direct sales volume might be explained by a deepening trust between long-time buyers and vendors, a growing distrust of darknet markets, a wish to avoid DNM fees, a desire to avoid being linked to known illicit activity, or some combination of these.

On average, these direct sales channels are substantial in terms of dollar amount: the average buyer sent a total of $8,441 worth of cryptocurrency to their preferred vendor during 2021. Sums this considerable may be indicative of large-scale illicit activity, whether it be attributed to drug trafficking or the sale of troves of financial data acquired through fraud.

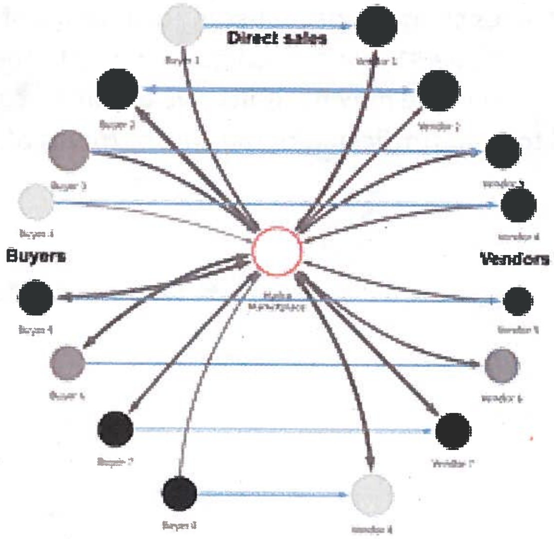
The median buyer, however, sent a total of just $603 to their preferred vendor this year.

Average and median value sent from each buyer to vendor per year | 2016-2021



This suggests that while massive direct sales account for a large majority of total volume, direct sales relationships exist at every size. In fact, this implies that more than half of all buyer-to-vendor relationships likely operate at a retail level, with the buyer sending less than $603 worth of cryptocurrency to the vendor during the year.

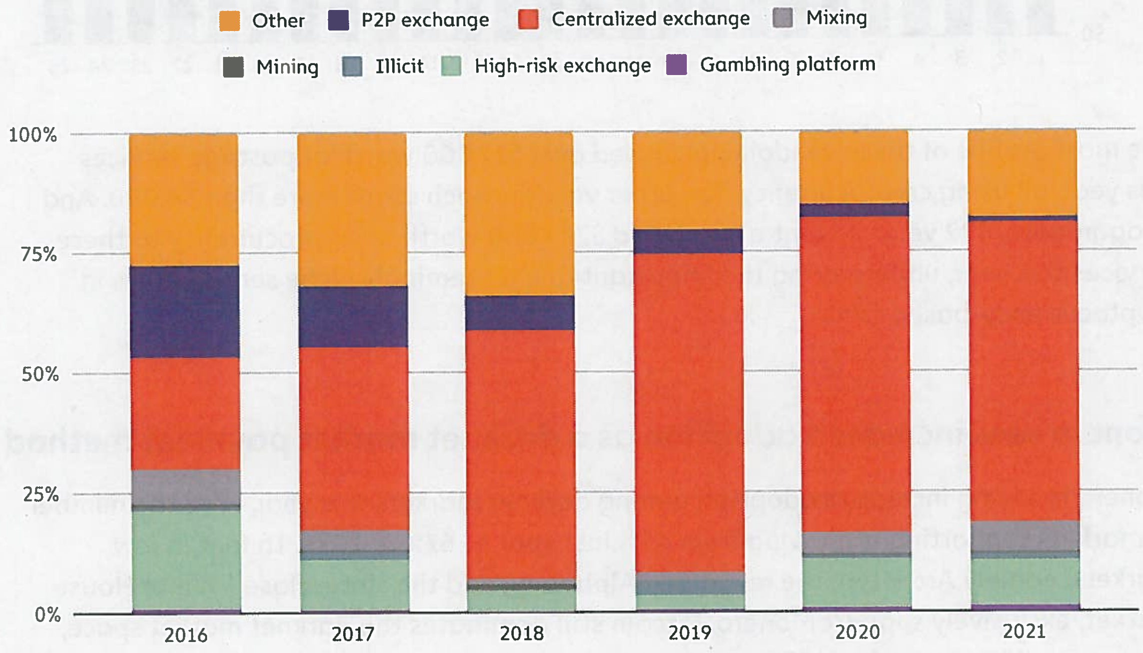
Nonetheless, the upper outliers are worth observing. Below, we visualize the eight largest buyer-to-vendor relationships by total value sent in 2021.



Each of these top buyers and vendors dealing directly have previously transacted through Hydra, presumably with one another (though we can't know for sure), as denoted by the grey lines. The blue lines, on the other hand, show direct transactions between the two without Hydra as an intermediary. On average, each buyer in this relationship has sent more than $3.1 million worth of cryptocurrency to their preferred vendor in 2021. This aligns with our hypothesis that the biggest direct relationships have ties to large-scale illicit activity.

We can analyze the transaction history of vendors like those shown above to better understand their money laundering strategy, based on the types of services to which they send funds.

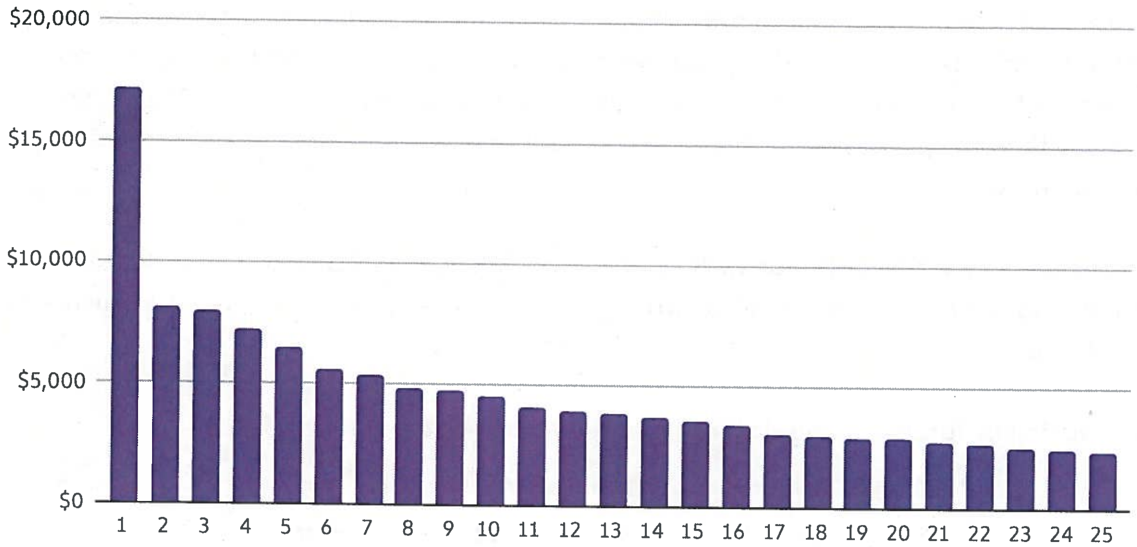
Destination of funds leaving darknet market vendor addresses | 2016-2021



Mainstream centralized exchanges are the most common destination, with high-risk exchanges and mixers also receiving a significant share.

Of course, not all funds sent from darknet market vendors indicate money laundering. Vendors often use cryptocurrency to purchase products and services necessary for their operations. Postage products and services — stamps, boxes, shipping labels, and the like — are a perfect example, as drug vendors typically mail their products to buyers. Chainalysis tracks several postage providers who accept payments in cryptocurrency, and has identified several darknet market vendors sending those providers significant sums.

Top darknet market vendors by value sent to postage providers | 2021



The most prolific of these vendors purchased over $17,000 worth of postage services this year, all using cryptocurrency. Ten other vendors each spent more than $4,000. And in aggregate, 322 vendors sent a combined $207,000 worth of cryptocurrency to these services this year, underscoring the important role a seemingly niche service plays in cryptocurrency-based crime.

Monero sees increased adoption as a darknet market payment method

Monero is seeing increased adoption among darknet markets this year, with the number of markets supporting it growing from 45% last year to 67% in 2021. In fact, a few markets, namely Archetyp, the revamped Alphabay, and the since-closed White House Market, exclusively support Monero. Bitcoin still dominates the darknet market space, however, with support from 93% of all markets.

Consolidation, competition, and caution defined darknet markets in 2021

Even as the demand for drugs and stolen credentials has continued to move online, competitors' black hat tactics and law enforcement takedowns have driven many more markets offline. In an abundance of caution, several markets have even closed voluntarily, while the markets that have opened in their place have embraced privacy-enhanced designs. Meanwhile, vendors have taken more steps than ever to enhance their shipping anonymity, and buyers have begun to transact with these vendors directly. All of these trends point to a darknet market industry that is fast maturing.

To solve cases that interface with darknet markets, investigators should be aware of these trends and have access to the proper tools to address them. Chainalysis Reactor's extensive attributions, graphing capabilities, and investigation teams can provide just that—the expertise and tooling needed to turn this blockchain data into actionable leads.

High-risk Jurisdictions & Sanctions

High-risk Jurisdictions & Sanctions

North Korea

North Korean Hackers Have Prolific Year as Their Total Unlaundered Cryptocurrency Holdings Reach All-time High

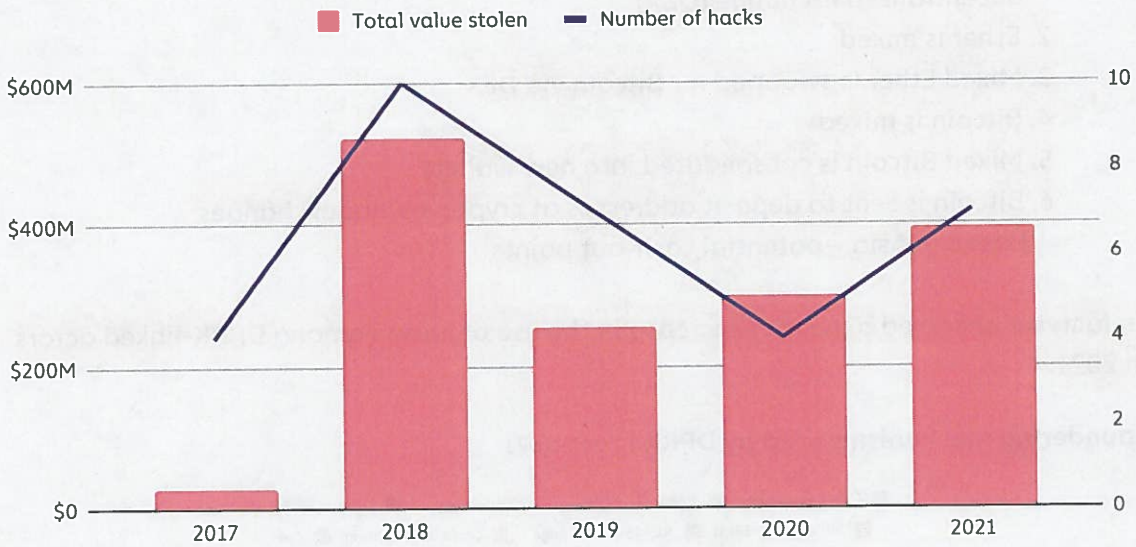
North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms that extracted nearly $400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' internet-connected "hot" wallets into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out.

These complex tactics and techniques have led many security researchers to characterize cyber actors for the Democratic People's Republic of Korea (DPRK) as advanced persistent threats (APTs). This is especially true for APT 38, also known as "Lazarus Group," which is led by DPRK's primary intelligence agency, the US- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.

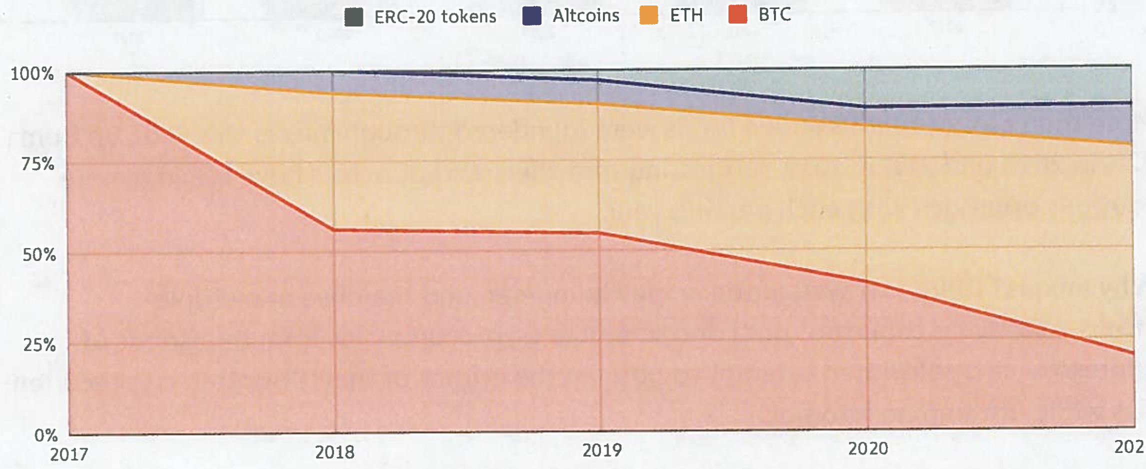
In 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%.

North Korean-linked hacks by total value stolen and total number of hacks | 2017–2021



Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the cryptocurrencies stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22% were either ERC-20 tokens or altcoins. And for the first time ever, Ether accounted for a majority of the funds stolen at 58%.

Share of funds stolen by DPRK by coin type | 2017–2021

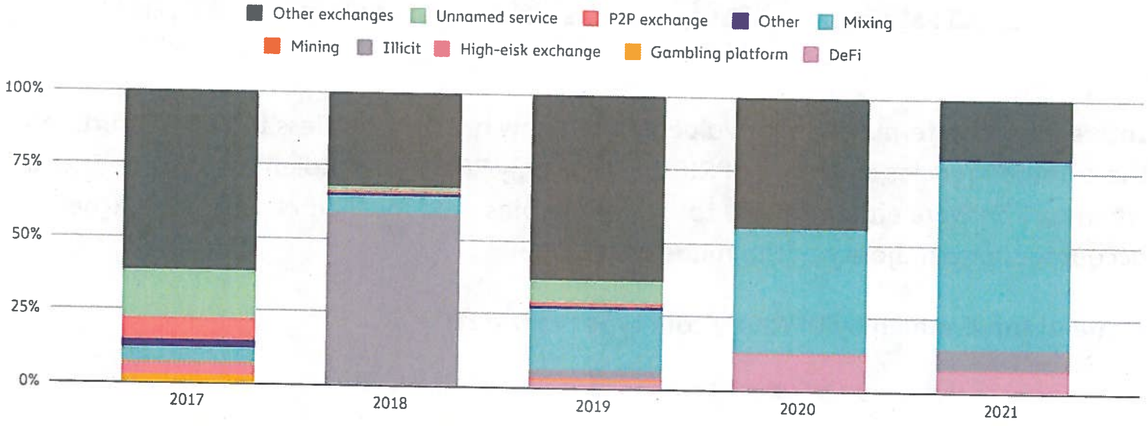


The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
2. Ether is mixed
3. Mixed Ether is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia —potential cash-out points

In fact, we observed a massive increase in the use of mixers among DPRK-linked actors in 2021.

Laundering mechanisms used by DPRK | 2017–2021



More than 65% of DPRK's stolen funds were laundered through mixers this year, up from 42% in 2020 and 21% in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year.

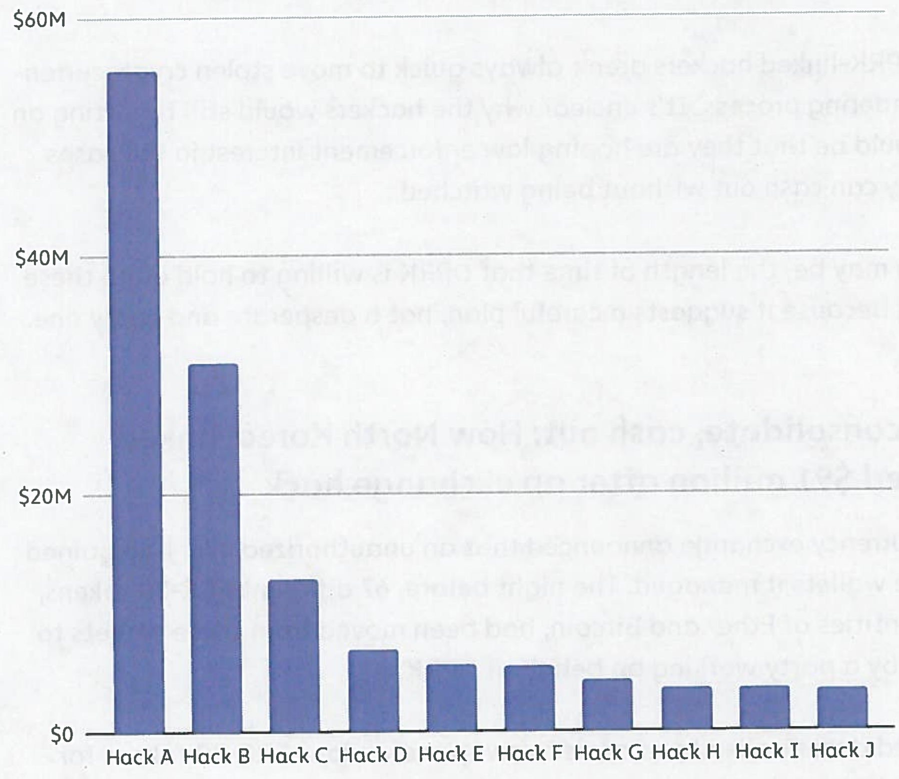
Why mixers? DPRK is a systematic money launderer, and their use of multiple mixers —software tools that pool and scramble cryptocurrencies from thousands of addresses—is a calculated attempt to obscure the origins of their ill-gotten cryptocurrencies while offramping into fiat.

Why DeFi? DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. What's more, DeFi platforms don't take custody of user funds and many do not collect know-your-customer (KYC) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed.

DPRK's stolen fund stockpile: $170 million worth of old, unlaundered cryptocurrency holdings

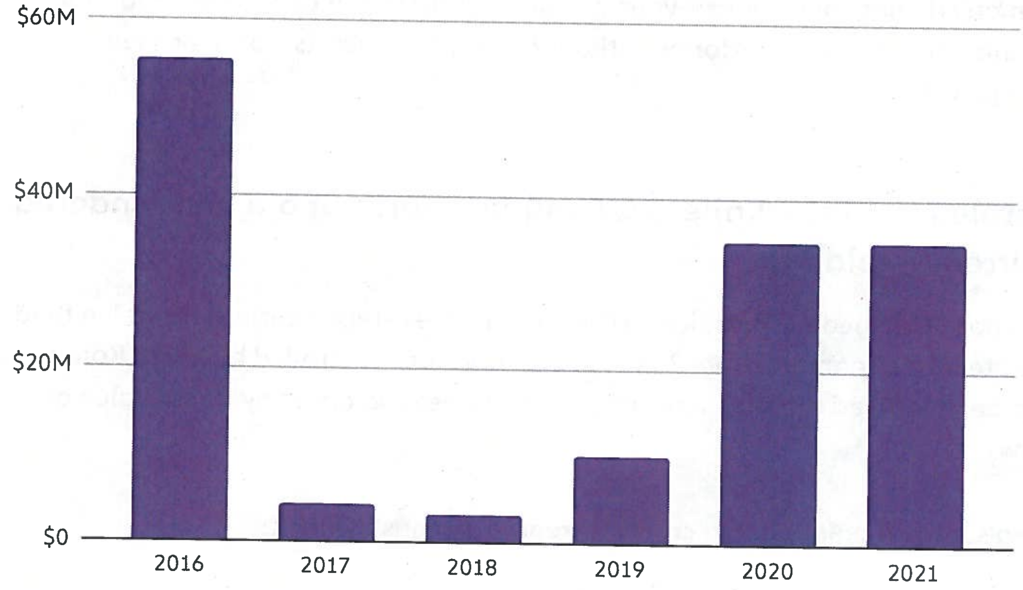
Chainalysis has identified $170 million in current balances—representing the stolen funds of 49 separate hacks spanning from 2017 to 2021—that are controlled by North Korea but have yet to be laundered through services. The ten largest balances by dollar value are listed below.

North Korea's largest unlaundered cryptocurrency holdings by hack



Of DPRK's total holdings, roughly $35 million came from attacks in 2020 and 2021. By contrast, more than $55 million came from attacks carried out in 2016—meaning that DPRK has massive unlaundered balances as much as six years old.

Total balances held by North Korean actors by date of attack | 2016–2021



This suggests that DPRK-linked hackers aren't always quick to move stolen cryptocurrencies through the laundering process. It's unclear why the hackers would still be sitting on these funds, but it could be that they are hoping law enforcement interest in the cases will die down, so they can cash out without being watched.

Whatever the reason may be, the length of time that DPRK is willing to hold on to these funds is illuminating, because it suggests a careful plan, not a desperate and hasty one.

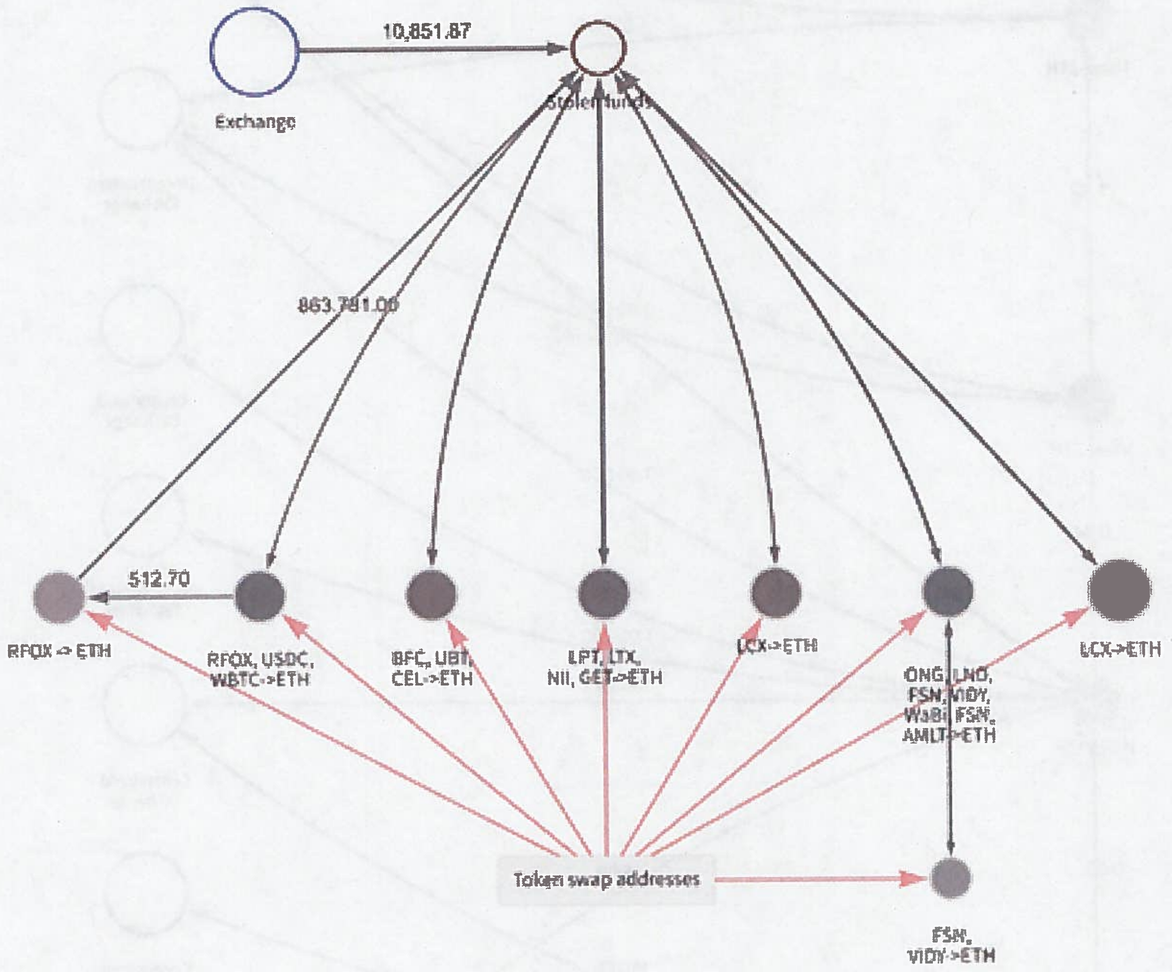
Coinswap, mix, consolidate, cash out: How North Korea-linked hackers laundered $91 million after an exchange hack

In August, a cryptocurrency exchange announced that an unauthorized user had gained access to some of the wallets it managed. The night before, 67 different ERC-20 tokens, along with large quantities of Ether and Bitcoin, had been moved from these wallets to addresses controlled by a party working on behalf of DPRK.

The attacker then used decentralized protocols to swap the various ERC-20 tokens for Ether. From there, they mixed the Ether, swapped the mixed Ether for Bitcoin, mixed the Bitcoin, consolidated the mixed Bitcoin into new wallets, and then deposited the funds into crypto-to-fiat exchanges based in Asia. As a result, approximately $91.35M in cryptoassets was laundered.

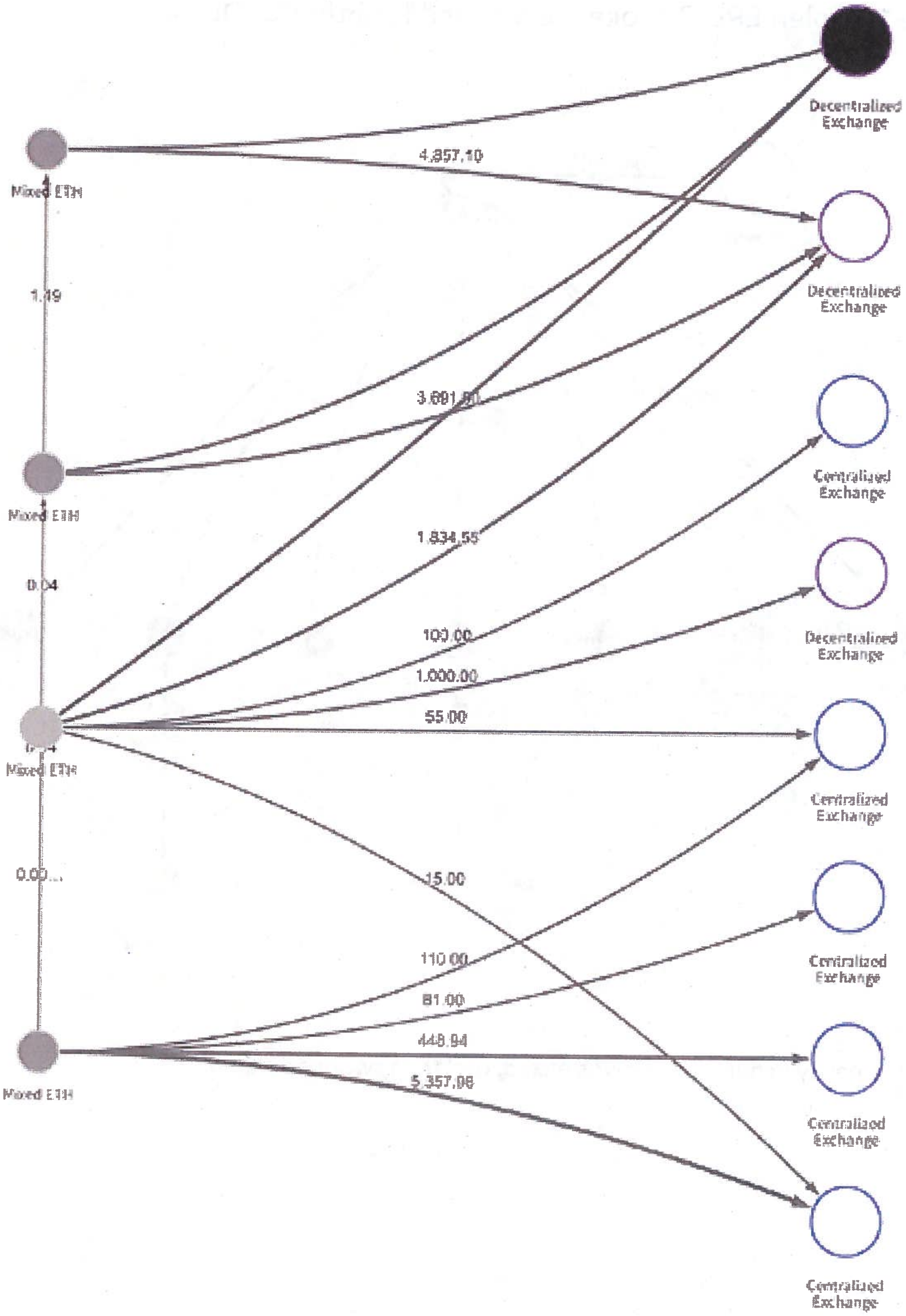
Below, we've visualized each stage of the laundering process in Chainalysis Reactor.

Stage 1: Stolen ERC-20 tokens swapped for Ether at DEXs:

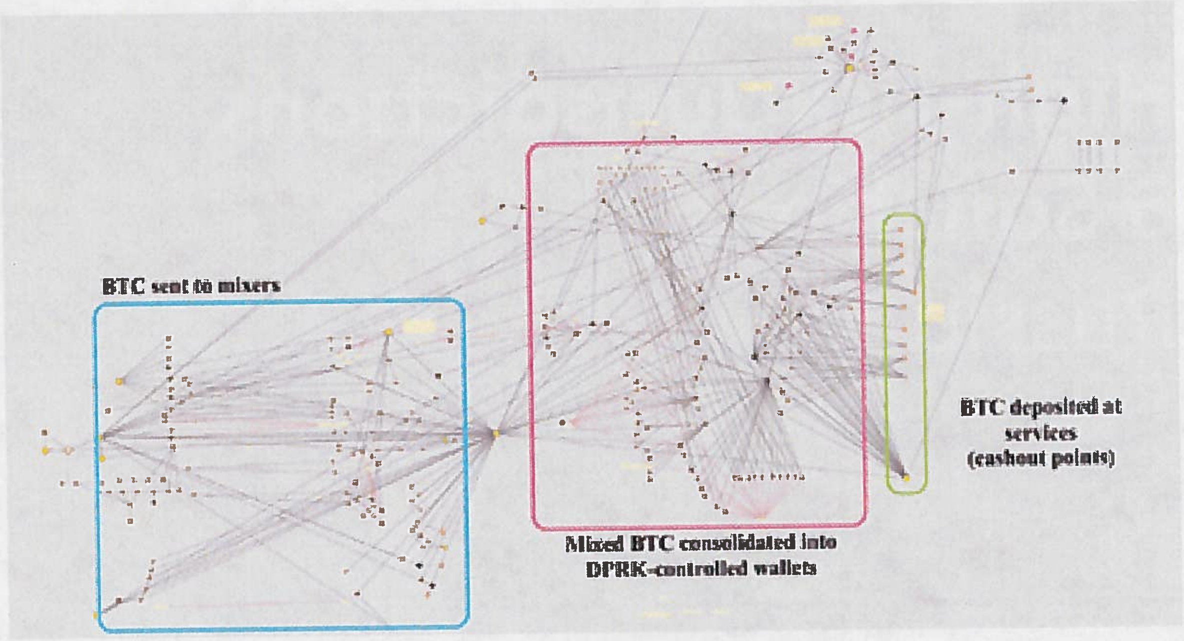


Next, the newly acquired Ether was mixed, and then swapped again.

Stage 2: Mixed Ether deposited at DEXs and CEXs to swap for Bitcoin



Stage 3: Movement of stolen funds after being swapped for BTC


BTC sent to mixers
Mixed BTC consolidated into DPRK-controlled wallets
BTC deposited at services (cashout points)

At the end of this process, the attackers move the Bitcoin to centralized, primarily Asia-based exchanges, where it's likely swapped for a fiat currency like China's Renminbi, allowing them to finally access the cash gained from the hack.

DPRK: An advanced persistent threat to the cryptocurrency industry

These behaviors, put together, paint a portrait of a nation that supports cryptocurrency-enabled crime on a massive scale. Systematic and sophisticated, North Korea's government—be it through the Lazarus Group or its other criminal syndicates—has cemented itself as an advanced persistent threat to the cryptocurrency industry in 2021.

Nonetheless, the inherent transparency of many cryptocurrencies presents a way forward. With blockchain analysis tools, compliance teams, criminal investigators, and hack victims can follow the movement of stolen funds, jump on opportunities to freeze or seize assets, and hold bad actors accountable for their crimes.

High-risk Jurisdictions & Sanctions

Russia

Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity

Russia is a leading country in cryptocurrency adoption, placing 18th overall on our Global Crypto Adoption Index. But the story of Russia's cryptocurrency usage isn't entirely positive. Individuals and groups based in Russia — some of whom have been sanctioned by the United States in recent years — account for a disproportionate share of activity in several forms of cryptocurrency-based crime.

In this section, we'll delve into two intertwined areas of Russia's crypto crime ecosystem that, together, have serious implications for cybersecurity, compliance, and national security: ransomware and money laundering.

Russian cybercriminals set the pace for ransomware

Russia has long been home to some of the most skilled hackers in the world. According to cybersecurity investigators like Brian Krebs, this is largely due to the country's excellence in computer science education, combined with low economic prospects even for those who are skilled in the field. Given this background, it may not be surprising that Russia leads the way in ransomware. But the degree to which Russia-based ransomware strains dominate is quite shocking.

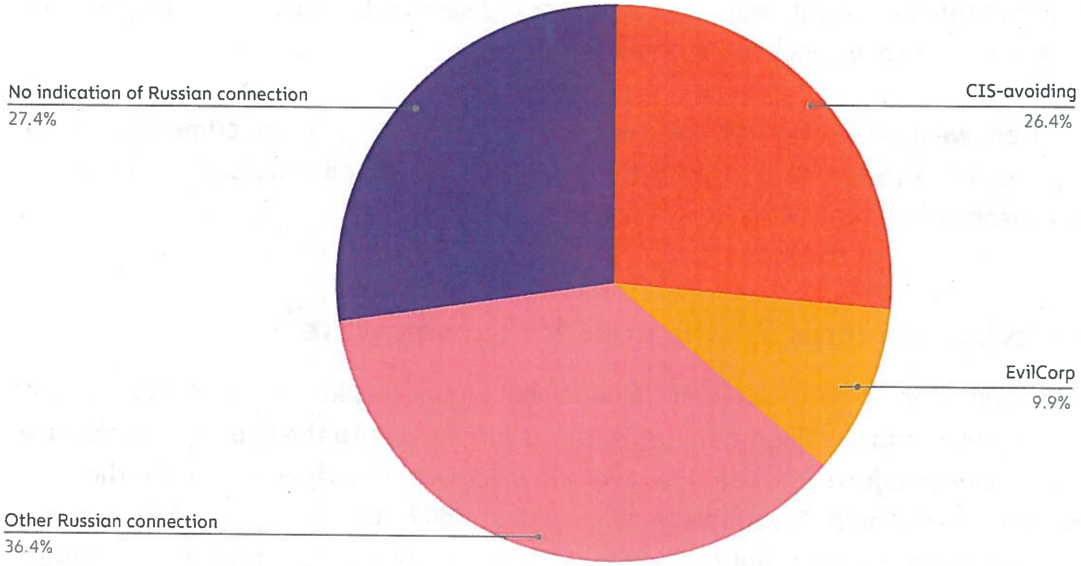
Before we dive into the data, a quick explainer — we generally tie specific ransomware strains to Russian cybercriminals based on one of three criteria:

- **Evil Corp.** Evil Corp is a Russia-based cybercriminal organization that has been prolific in ransomware, and whose leadership is believed to have ties to the Russian government.
- **Avoids CIS countries.** The Commonwealth of Independent States (CIS) is an intergovernmental organization of Russian-speaking, former Soviet countries. Many ransomware strains contain code that prevents the encryption of files if it detects the victim's operating system is located in a CIS country. In other cases, ransomware operators have even given over decryptors to return file access after learning they inadvertently targeted a Russian organization. We can attribute CIS-avoiding strains to Russian cybercriminals, though with a lesser degree of confidence, as some of them may be based in other CIS countries.
- **Other connections: language, affiliate location, etc.** There are several other ransomware characteristics that can indicate a strain is likely based in Russia. Examples include ransomware strains that share documents and announcements

in the Russian language, or whose affiliates are believed to be located in Russia with a high degree of confidence.

Using those three criteria, we show on the pie chart below the share of total ransomware revenue that went to strains affiliated with Russian organizations in 2021.

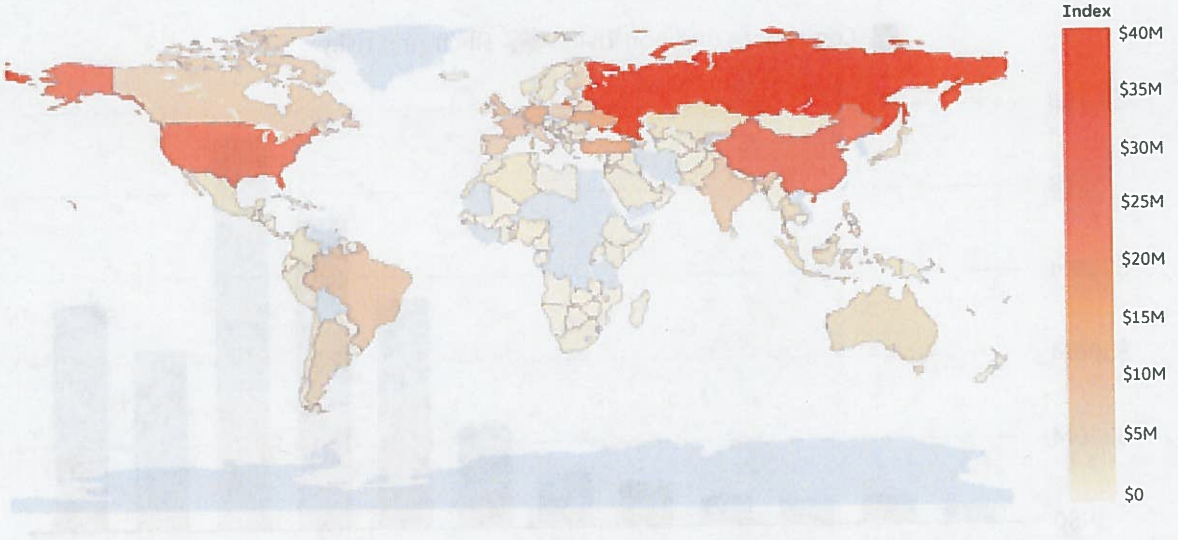
Share of 2021 ransomware revenue taken by Russia-affiliated strains | 2021



Overall, roughly 74% of ransomware revenue in 2021 — over $400 million worth of cryptocurrency — went to strains we can say are highly likely to be affiliated with Russia in some way.

Blockchain analysis combined with web traffic data also tells us that after ransomware attacks take place, most of the extorted funds are laundered through services primarily catering to Russian users.

Estimation of regional exposure to ransomware funds | 2021

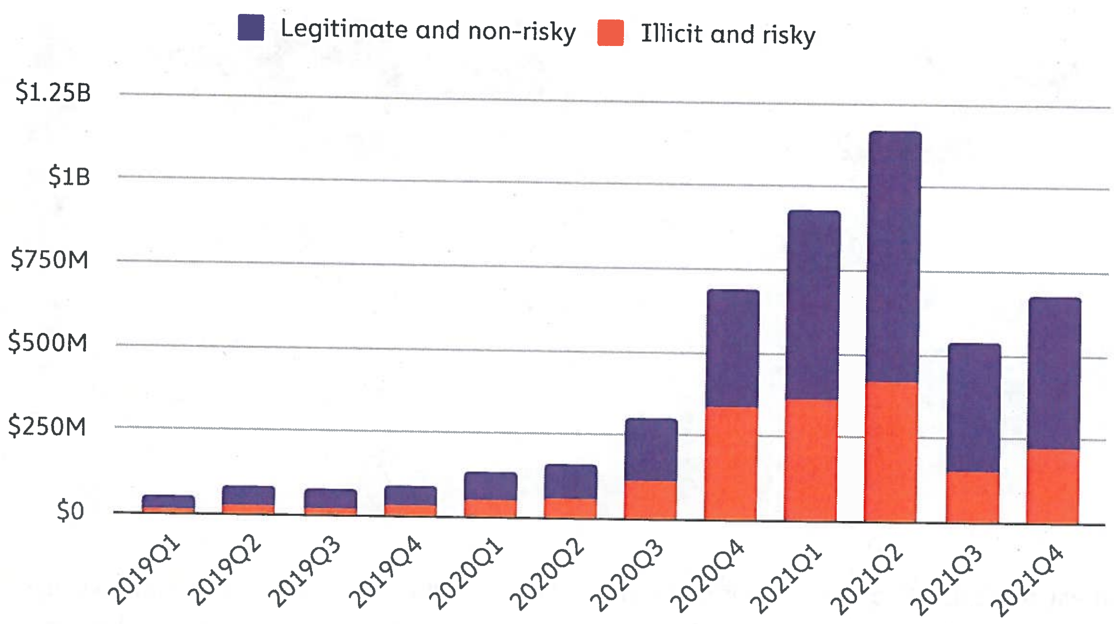


An estimated 13% of funds sent from ransomware addresses to services went to users estimated to be in Russia, more than any other region. That brings us to another point: A huge amount of cryptocurrency-based money laundering, not just of ransomware funds but of funds associated with other forms of cybercrime as well, goes through services with substantial operations in Russia.

Cryptocurrency-based money laundering in Moscow City

Russia is home to several cryptocurrency businesses that have processed substantial transaction volume from illicit addresses. In order to illustrate the scope of the problem, we thought it would be interesting to zoom in on businesses headquartered or with a significant presence in the capital's financial district, Moscow City. Chainalysis is tracking several dozen cryptocurrency businesses operating in Moscow City alone that facilitate significant amounts of money laundering.

Total value received by Moscow City cryptocurrency buinesses | 2019–2021

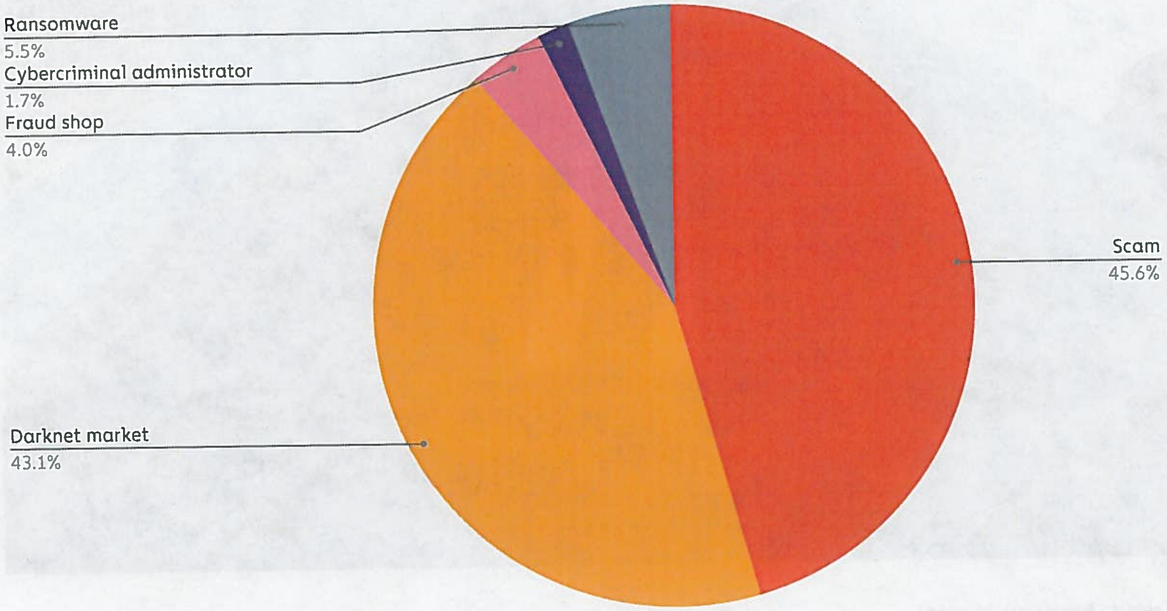


Note: The word "risky" here defines addresses connected to entities that, while not necessarily inherently criminal, are frequently linked to criminal activity, such as high-risk exchanges and mixers.

Collectively, these businesses receive hundreds of millions of dollars' worth of cryptocurrency per quarter, with totals peaking at nearly $1.2 billion in the second quarter of 2021. In any given quarter, the illicit and risky addresses account for between 29% and 48% of all funds received by Moscow City cryptocurrency businesses. In total, across the three-year period studied, these businesses have received nearly $700 million worth of cryptocurrency from addresses associated with explicitly criminal activity, which represents 13% of all value they've received in that time. Where do these illicit funds come from?

Illicit cryptocurrency moving to Moscow cryptocurrency businesses by crime type

| 2019–2021

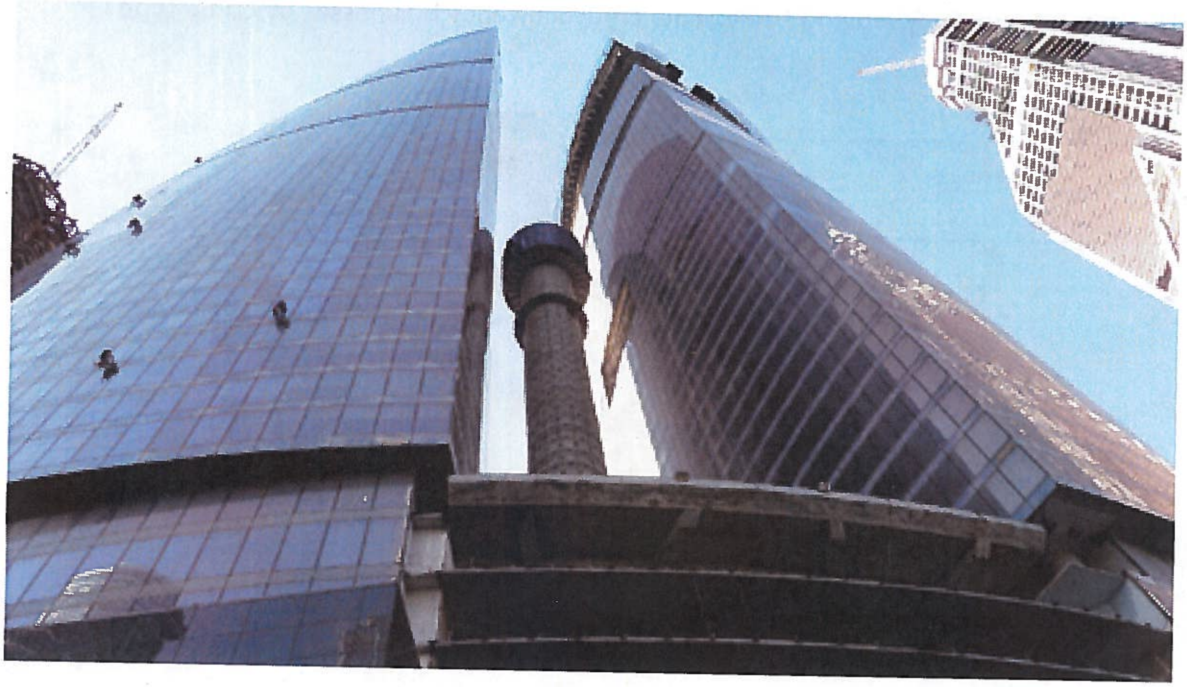


Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

Scams at $313 million and darknet markets at $296 million make up the vast majority of illicit cryptocurrency sent to the Moscow City cryptocurrency businesses we track between 2019 and 2021. Ransomware is third at $38 million.

Overall, the Moscow City cryptocurrency businesses we track vary greatly in the role that money laundering plays in their overall business. Some of them are big enough that despite receiving millions of dollars' worth of funds from illicit addresses, those funds only represent 10% or less of all cryptocurrency they receive. Those instances could be attributed to the business's lack of knowledge, rather than purposeful criminal activity. But for other Moscow City cryptocurrency businesses, illicit funds make up as much as 30% or more of all cryptocurrency received, which suggests those businesses may be making a concerted effort to serve a cybercriminal clientele.

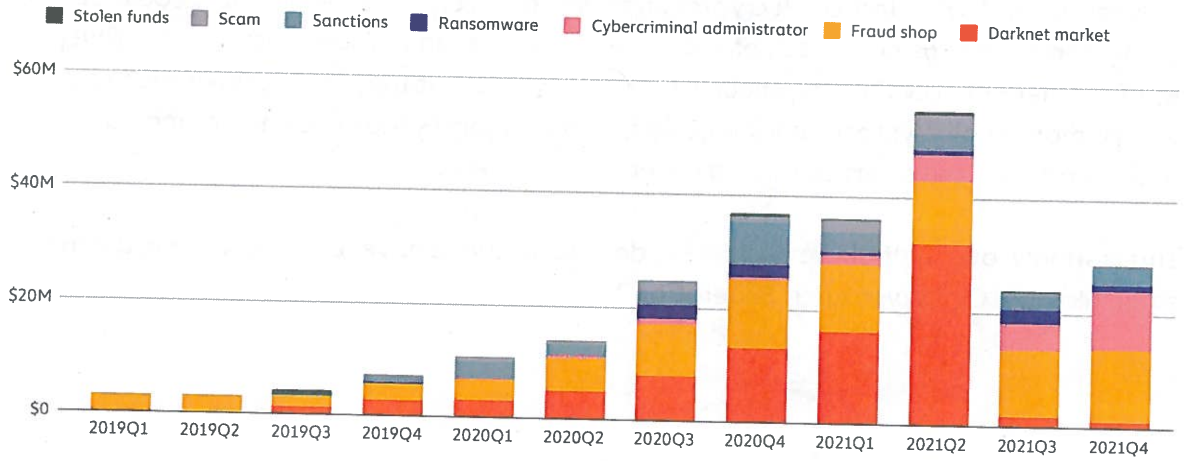
Interestingly, over half of the businesses described above have reportedly operated in the same Moscow City skyscraper: Federation Tower.



Credit: Mariano Mantel

Federation Tower, a two skyscraper complex in the heart of Moscow City, is one of the most prestigious buildings in all of Russia, with several prominent businesses headquartered there and residential units going for upwards of $36 million. However, as outlets like Bloomberg and the New York Times have reported, Federation Tower is home to several cryptocurrency businesses that have facilitated extensive money laundering, accepting funds from addresses involved in various forms of cryptocurrency-based crime — especially scams, darknet markets, and ransomware.

Illicit funds moving to Federation Tower cryptocurrency businesses | 2019–2021



Nothing is more emblematic of the growth of Russia's crypto crime ecosystem, and of cybercriminals' ability to operate with apparent impunity, than the presence of so many cryptocurrency businesses linked to money laundering in one of the capital city's most notable landmarks.

Below, we highlight some of the cryptocurrency businesses with a presence in Moscow City that have facilitated the most money laundering or are otherwise notable:

Analysis of a selection of Moscow City cryptocurrency businesses facilitating money-laundering | 2019–2021

Name	Total cryptocurrency value received (2019–2021)	Illicit and risky cryptocurrency value received (2019–2021)	Share of all value received coming from illicit and risky sources (2019–2021)	Notes
Garantex	$2,114,431,000	$645,223,700	31%	Has received over $10 million from ransomware strains including NetWalker, Phoenix Cryptolocker, and Conti.
Eggchange	$34,081,220	$3,705,827	11%	Has received hundreds of thousands of dollars' worth of cryptocurrency from darknet markets, scams, fraud shops, and ransomware operators. Founder Denis Dubnikov was arrested for his alleged role in helping Ryuk ransomware operators launder funds.
Cashbank	$45,400,600	$180,119	0.4%	While Cashbank's detected money laundering activity is relatively low in volume, it advertises on forums frequented by illicit actors and criminals.
Buy-bitcoin	$41,604,170	$11,374,910	27%	Has received $2.1 million from darknet markets, $400,000 in stolen funds, and $400,000 from ransomware attackers.
Tetchange	$21,903,700	$4,621,440	21%	Has received over $1 million from darknet markets and $600,000 from ransomware attackers.

Bitzlato	$2,000,077,000	$966,254,800	48%	Has received $206 million from darknet markets, $224.5 million from scams, and $9 million from ransomware attackers.
Suex	$426,189,500	$158,856,100	37%	Has received $24 million from scams, $20 million from darknet markets, and $12 million from ransomware. Sanctioned by OFAC in 2021.

What's next for crypto crime in Russia?

Looking ahead, change may be on the way for Russia's cryptocurrency ecosystem, especially as it relates to crime. In January 2022, Russian police arrested 14 affiliates of the REvil ransomware organization, marking one of the only times the local authorities have taken action against ransomware attackers operating within the country. However, analysts have speculated that the arrests were an act of diplomacy meant to cool tensions with the United States over Russia's troop buildup on Ukraine's borders, and may not indicate true commitment to fighting ransomware. At the same time, cryptocurrency's regulatory status in Russia appears to be in flux, with President Vladimir Putin defending cryptocurrency miners at the same time the country's national bank recommends an all-out ban on all cryptocurrency activity.

Regardless of what the future holds, it's important to understand where things stand now: Russian cybercriminal organizations are some of the biggest perpetrators of cryptocurrency-based crime — especially ransomware — and local cryptocurrency businesses provide money laundering services that enable this activity. 2021 saw positive momentum against this issue, from the seizure of funds from ransomware organization DarkSide to the sanctioning of Suex and Chatex. Chainalysis looks forward to working with law enforcement, regulators, and compliance professionals in 2022 to keep that momentum going.

Cryptocurrency Money Laundering in Moscow City

Together, these six Moscow City crypto services received $1.8 billion from addresses associated with illicit and risky activity.

Garantex

$645,223,700 recieved from illicit and risky sources

31% of all value received

Buy-bitcoin

$11,374,910 recieved from illicit and risky sources

27% of all value received

Bitzlato

$966,254,800 recieved from illicit and risky sources

48% of all value received

Eggchange

$3,705,827 recieved from illicit and risky sources

11% of all value received

Tetchange

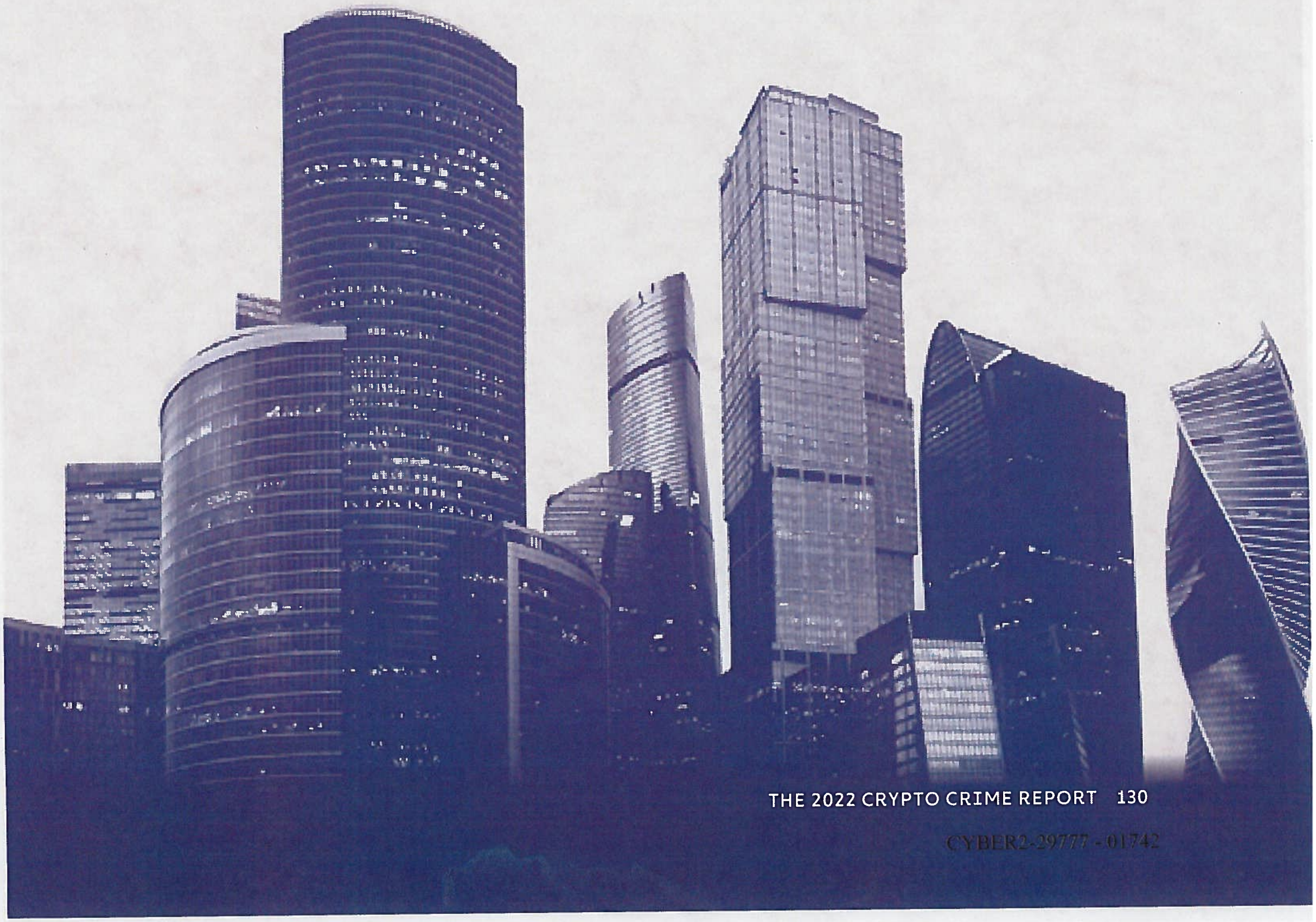
$4,621,440 recieved from illicit and risky sources

21% of all value received

Suex

$158,856,100 recieved from illicit and risky sources

37% of all value received



High-risk Jurisdictions & Sanctions

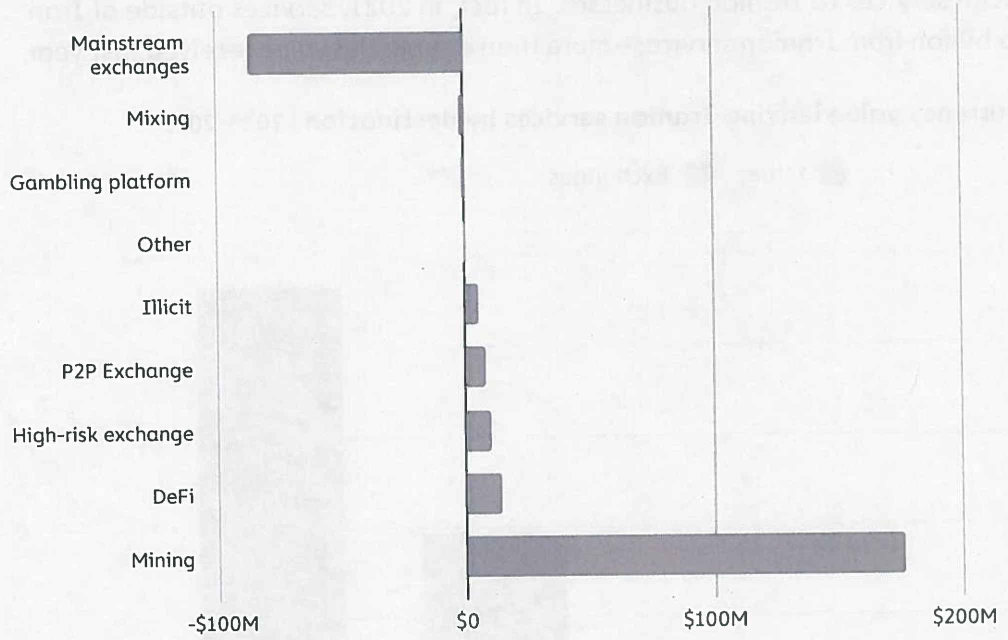
Iran

Bitcoin Mining Fuels Iran's Billion-Dollar Sanctions Evasions

Iran faces some of the most extensive U.S. sanctions of any country. Per the United States Treasury's Office of Foreign Assets Control (OFAC), U.S. businesses and individuals are effectively banned from transacting with Iranian businesses, including its biggest financial institutions and central bank. Some in the Iranian government have called for the country to use cryptocurrency to circumvent these sanctions, and Bitcoin mining may provide the perfect opportunity to do so. As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine cryptocurrencies like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop.

Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year.

Net flows to and from Iranian services | 2015–2021



Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for cryptocurrency mining. And in March 2021, a think tank tied to the President's office released a report stressing its benefits.

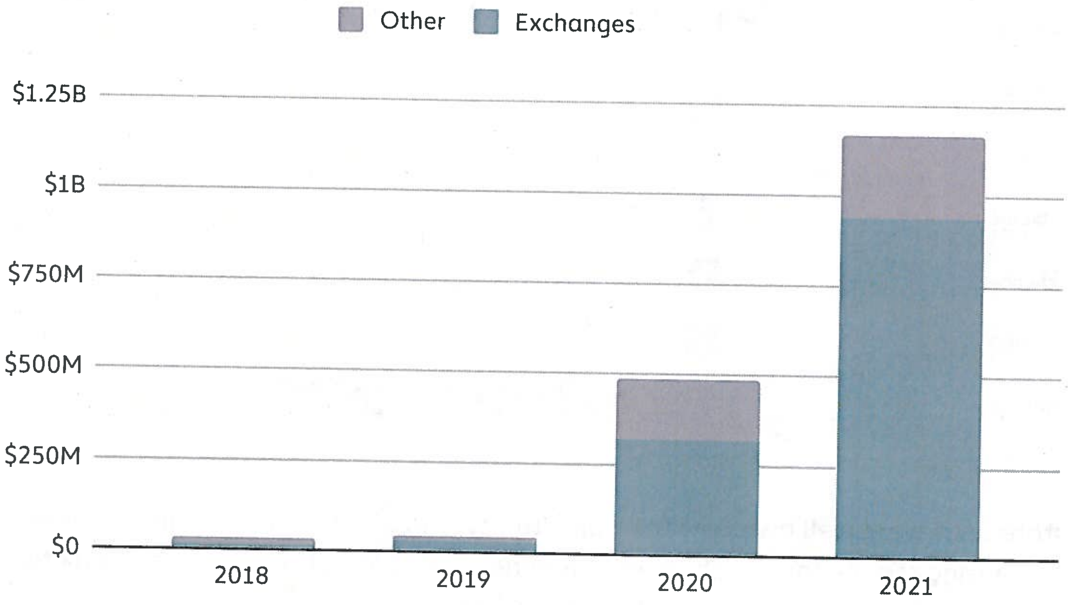
But the costs have extended beyond just electricity. The Iranian government has had to ban Bitcoin mining twice this year due to frequent blackouts, many of which Iran's state power agency has blamed on unlicensed Bitcoin mining. And unlicensed Bitcoin miners, for their part, allegedly account for "some 85%" of all activity in the country, per the Iranian president.

It has also opened up a new avenue of risk for cryptocurrency businesses. In theory, U.S. businesses could face penalties or even criminal prosecution if found in violation of OFAC sanctions, which prohibit U.S. persons or companies from servicing financial accounts belonging to Iranian persons or companies. That being said, businesses can monitor for exposure to Iranian miners to reduce this risk considerably.

It's also important to note that a nexus to sanctions is more attenuated at the transaction/mining fee level. If a U.S. business were to engage in a transaction and the fees paid from said transaction were received by an Iranian miner, the payer and payee would have had no say in who could receive these fees—the receiver of which is determined automatically by Bitcoin's proof-of-work protocol. To date, sanctions risk appears most prominent when a U.S. business transacts directly with the miner themselves.

Many exchanges operating in jurisdictions without active sanctions, however, continue to provide financial services to Iranian businesses. In fact, in 2021, services outside of Iran received $1.16 billion from Iranian services—more than double the value received last year.

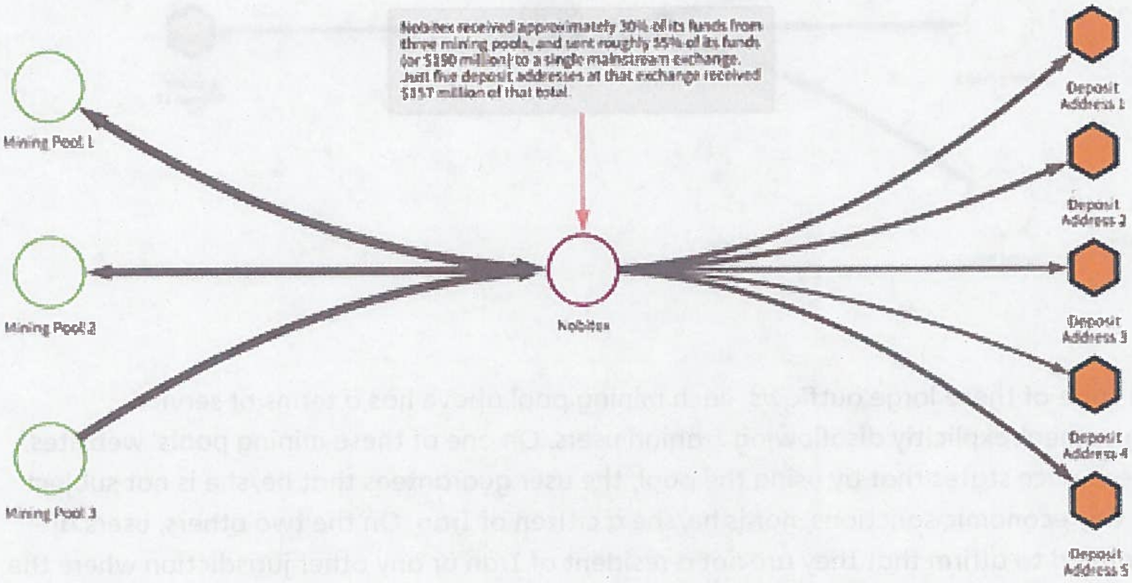
Total cryptocurrency value leaving Iranian services by destination | 2018–2021



This transfer of funds from mining pools to Iranian services to services in the wider cryptocurrency ecosystem is a key corridor through which Iran evades sanctions. In the next section, we illustrate the most common paths to this end.

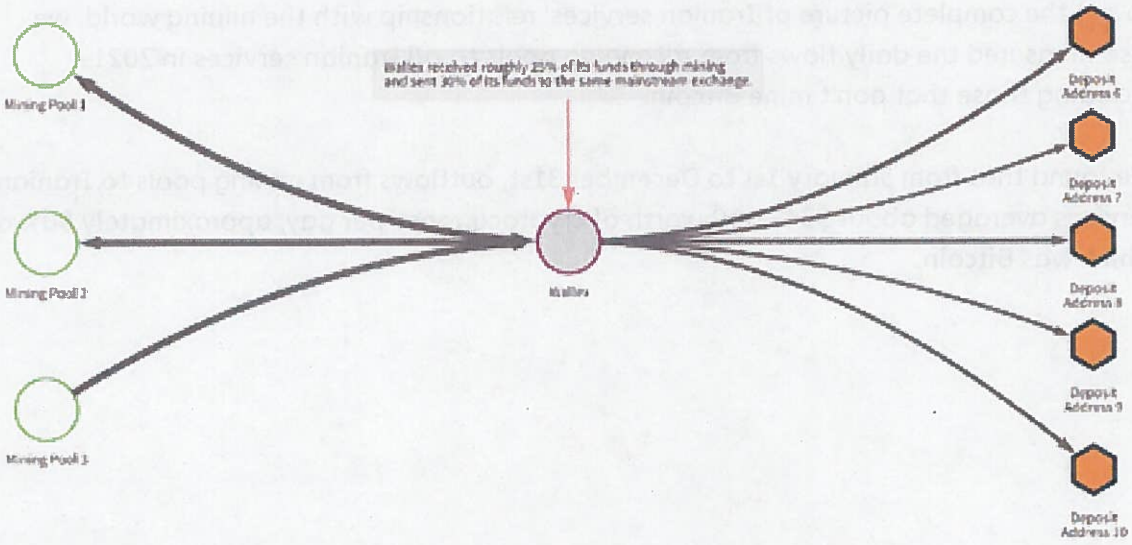
From mining pools to mainstream exchanges: Iran's sanctions evasion visualized

We can identify several of the services enabling Iran's sanctions evasion with blockchain analysis. Using Chainalysis Reactor, we visualize below the flow of funds from three mining pools to one mainstream exchange by way of Nobitex.ir, Iran's largest cryptocurrency exchange.



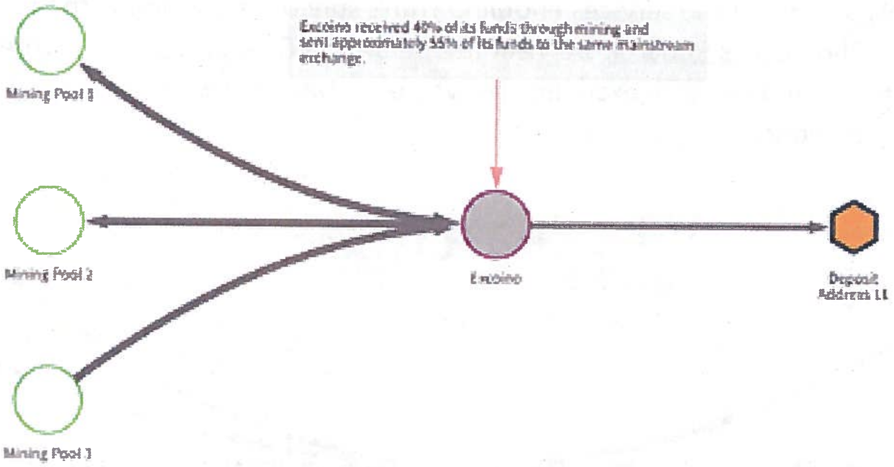
Nobitex received approximately 30% of its funds from three mining pools, and sent roughly 35% of its funds (or $150 million) to a single mainstream exchange. Just five deposit addresses at that exchange received $157 million of that total.

These same pools have similar degrees of exposure to Iran's second largest exchange, Wallex.ir.



Wallex received roughly 25% of its funds through mining and sent 30% of its funds to the same mainstream exchange.

And similar degrees of exposure to Iran's third largest exchange, Excoino.com.



Excoino received 40% of its funds through mining and sent approximately 55% of its funds to the same mainstream exchange.

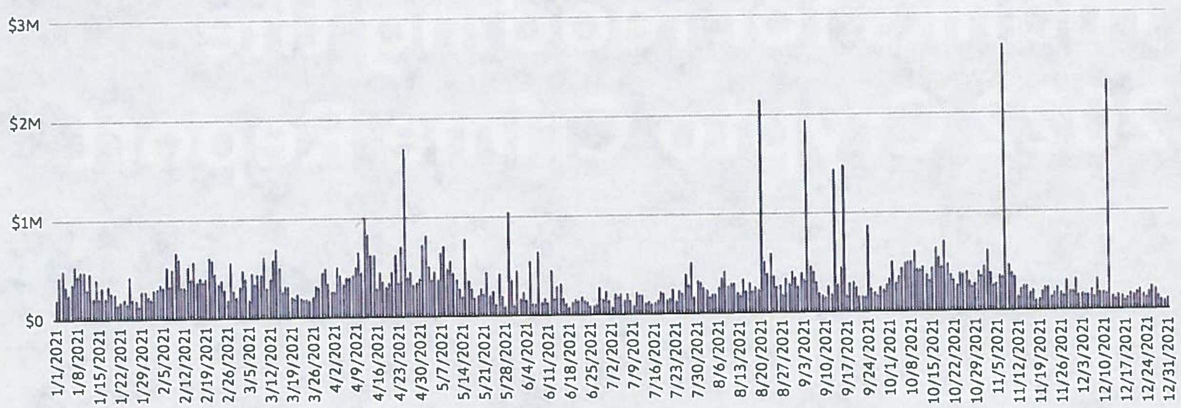
In spite of these large outflows, each mining pool above has a terms of service agreement explicitly disallowing Iranian users. On one of these mining pools' websites, the service states that by using the pool, the user guarantees that he/she is not subject to any economic sanctions, nor is he/she a citizen of Iran. On the two others, users are required to affirm that they are not a resident of Iran or any other jurisdiction where the services provided are restricted.

However, each mining pool above continues to send funds to Iranian services as of this report's release.

To get the complete picture of Iranian services' relationship with the mining world, we also measured the daily flows from *all* mining pools to *all* Iranian services in 2021—including those that don't mine Bitcoin.

We found that from January 1st to December 31st, outflows from mining pools to Iranian services averaged about $343,000 worth of cryptocurrency per day, approximately 80% of which was Bitcoin.

Daily cryptocurrency value received by Iranian services from mining pools | 2021



Interpreting these findings

Since our model captures only those mining pools with sending exposure to Iranian services in particular, $186 million likely underestimates Iran's total Bitcoin mining revenue from 2015 to 2021. In fact, other mining pools may support *much more* Iranian mining activity than the three pools we identify here—and given Iran's estimated 3.11% monthly share of the global hashrate, this is probably true. As such, this estimate should be considered a lower bound.

The implications for government agencies, financial institutions, and cryptocurrency businesses

With Iran embracing cryptocurrency, we advise interested government agencies to watch this situation closely. To avoid the risk of sanctions violations, we encourage U.S. cryptocurrency businesses and financial institutions to do the same. Businesses can automatically monitor for transactional exposure to Iranian entities with Chainalysis KYT, while government agencies can identify these transactions' counterparties with Reactor.

Thanks for reading the 2022 Crypto Crime Report

Chainalysis Authors

Kim Grauer
Director of Research

Will Kueshner
Content Marketer

Henry Updegrave
Senior Content Marketing Manager

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making investment decisions.

This report contains links to third-party sites that are not under the control of Chainalysis, Inc. or its affiliates (collectively "Chainalysis"). Access to such information does not imply association with, endorsement of, approval of, or recommendation by Chainalysis of the site or its operators, and C hainalysis is not responsible for the products, services, or other content hosted therein.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.

Chainalysis

Check out more original Chainalysis research

Chainalysis Reports

Cryptocurrency Exchanges in 2021: A Competitive Analysis

The 2021 NFT Market Report: Everything You Need to Know About the NFT Market and Its Most Successful Collectors

VIEW ALL REPORTS

Chainalysis Insights

Data-driven content on cryptocurrency markets, regulation and developments

VISIT THE BLOG

Chainalysis

Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Our data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Coatue, Paradigm, Ribbit, and other leading firms in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit www.chainalysis.com.

GET IN TOUCH
info@chainalysis.com

FOR MORE CONTENT
visit blog.chainalysis.com

FOLLOW US ON TWITTER
@chainalysis

FOLLOW US ON LINKED IN
/chainalysis

EXHIBIT 179

U.S. Department of Justice

REPORT OF THE ATTORNEY GENERAL'S

CYBER DIGITAL TASK FORCE

CRYPTOCURRENCY

ENFORCEMENT FRAMEWORK

REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE

United States Department of Justice
Office of the Deputy Attorney General
Cyber-Digital Task Force
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
https://www.justice.gov/cryptoreport

October 2020

* * *

Guidance Disclaimer: This document does not contain any new binding legal requirements not otherwise already imposed by statute or regulation. To the extent this Enforcement Framework is viewed as a guidance document within the definition of Executive Order 13891, the contents of this document do not have the force and effect of law and are not meant to bind the public in any way. If viewed as a guidance document, this document is intended only to provide clarity to the public regarding existing requirements under the law or Department of Justice policies.

Table of Contents

ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE

Task Force Members

Sujit Raman, Chair
Associate Deputy Attorney General
Office of the Deputy Attorney General

John Brown
Executive Assistant Director
Federal Bureau of Investigation

John C. Demers
Assistant Attorney General
National Security Division

Andrew E. Lelling
United States Attorney
District of Massachusetts

Brian C. Rabbitt
Assistant Attorney General (Acting)
Criminal Division

Terry Wade
Executive Assistant Director
Federal Bureau of Investigation

Beth A. Williams
Assistant Attorney General
Office of Legal Policy

Task Force Contributors

Anthony M. Shults
Senior Counsel, Office of Legal Policy
Staff Director

Sabrina Bagdasarian
Jeff Breinholt
Thomas Burrows
Richard W. Downing

Lindsey Freeman
Christopher Hardee
Adam Hickey
Michele R. Korver
Erin Mikita

Sean Newell
C. Alden Pelker
Kimberley Raleigh
Leo Tsao

And the Men and Women of the Federal Bureau of Investigation

Introduction

Innovation can drive a society forward. But innovation does not occur in a vacuum. Public policy can establish background conditions that help the innovative spirit thrive—or create an environment in which that spirit is inhibited, or suppressed.

Even in societies where transformative scientific and technological advancements are achievable, public policy again plays a critical mediating role. In the wrong hands, or without appropriate safeguards and oversight, these advancements can facilitate great human suffering. Just ask the political enemies of authoritarian regimes that deploy surveillance tools Orwell never could have imagined. Or, closer to home, listen to the child victims of unspeakable sexual exploitation whose images and livestreamed abuse are so easily transmitted across the internet.

Technological innovation and human flourishing are complementary concepts, but the former does not guarantee the latter. Good public policy—and the fair and equitable enforcement of such policy—can help bring the two into alignment. And even as too much regulation undoubtedly stifles innovation (and human flourishing, too), the absence of law's protections can endanger progress across both dimensions. It takes careful consideration, and a deep and ongoing immersion in the facts, to understand when, and how, law should intervene. Once law's empire has established its root in a particular domain, it requires equally careful consideration (and humility on the part of government officials) to ensure that regulation goes no further than is required—that government action, in other words, reflects enforcement only of "those wise restraints that make us free."[i]

This Enforcement Framework

In 2018, Attorney General Jeff Sessions established a Cyber-Digital Task Force within the U.S. Department of Justice to evaluate the impact that recent advances in technology have had on law enforcement's ability to keep our citizens safe. Acknowledging the many ways in which technological advances "have enriched our lives and have driven our economy," the Attorney General also noted that "the malign use of . . . technolog[y] harms our government, victimizes consumers and businesses, and endangers public safety and national security."[ii]

The Task Force issued a comprehensive report later that year. That report identified particular threats currently confronting our society, ranging from transnational criminal enterprises' sophisticated cyber-enabled schemes, to malign foreign influence operations, to efforts to compromise our nation's critical infrastructure. The report also identified a number of emerging threats whose contours are still developing, and recommended further examination of their potential impact. Specifically, the report recommended that "the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."[iii] This Cryptocurrency Enforcement Framework represents the fruits of the Task Force's efforts.

At the outset, it bears emphasizing that distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing. These possibilities are rightly being explored around the globe, from within academia and industry, and from within governments—including our own.

It should be no surprise, for example, that researchers within the U.S. National Institute of Standards and Technology "have been investigating blockchain technologies at multiple levels: from use cases, applications and existing services, to protocols, security guarantees, and cryptographic mechanisms."[iv] Or that the U.S. Department of Defense's recently-issued Digital Modernization Strategy specifically identifies blockchain technology as having "promise to provide increased effectiveness, efficiency, and security."[v] Or that the U.S. Food and Drug Administration recently released a detailed vision for how it plans to deploy blockchain for food safety-related purposes.[vi] Or that—in the cryptocurrency space specifically—"the Federal Reserve is active in conducting research and experimentation related to distributed ledger technologies and the potential use cases for digital currencies," including by partnering with the Massachusetts Institute of Technology to "build and test a hypothetical digital currency oriented to central bank uses."[vii] Without doubt, cryptocurrency represents a transformative way to store and exchange value.

But as the following pages make clear, despite its relatively brief existence, this technology already plays a role in many of the most significant criminal and national security threats our nation faces. As the Task Force has found, illicit uses of cryptocurrency typically fall into three categories: (1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself. Part I of this Enforcement Framework examines in detail each of those categories.

Our society is not powerless in the face of these threats. As Part II demonstrates, the government has legal and regulatory tools available at its disposal to confront the threats posed by cryptocurrency's illicit uses. Interagency partnership is critical for effectively leveraging those tools. The Department of Justice has built strong working relationships with its regulatory and enforcement partners in the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the U.S. Department of the Treasury (including FinCEN, OFAC, and the IRS), among others, to enforce federal law in both its civil and criminal aspects. We have actively participated in international regulatory and criminal enforcement efforts, as well.

Those efforts are paying off. The past year alone has witnessed the indictment and arrest of the alleged operator of the world's largest online child sexual exploitation market, involving an enforcement action that was coordinated with the disruption of that darknet market, the rescue of over 20 child victims, and the seizure of hundreds of thousands of dollars' worth of bitcoin; the largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns running into the millions of dollars involving Hamas's military wing, al-Qaeda, and ISIS; the first-ever imposition of economic sanctions for virtual-asset-related malicious cyber activity; and a novel (and successful) use of the federal securities laws to protect investors in the cryptocurrency space, resulting in the disgorgement of over $1.2 billion in ill-gotten gains in a single case. We expect these enforcement trends to continue.

This report concludes in Part III with a discussion of the ongoing challenges the government faces in cryptocurrency enforcement—particularly with respect to business models (employed by certain cryptocurrency exchanges, platforms, kiosks, and casinos), and to activity (like "mixing" and "tumbling," "chain hopping," and certain instances of jurisdictional arbitrage) that may facilitate criminal activity.

The Challenges We Face

Those challenges map neatly onto the broader set of challenges that many emerging technologies present to law enforcement. Blockchain-related technologies are complex and are difficult to learn; for example, the methods for executing crimes like pump-and-dump schemes are changing, and require investigators to familiarize themselves with everything from how initial coin offerings (ICOs) are conducted to how technologically-savvy people communicate on specialized communications applications. Not only are these emerging technologies difficult to learn, but the relevant markets also rapidly evolve. The ICO boom from a few years ago has given way to the exponential growth of Decentralized Finance markets in recent months—with all the associated complexities and difficulties for enforcers seeking to stay ahead of the curve and keep investors safe.

The global nature of the blockchain ecosystem adds a further layer of complexity. Crime has been expanding beyond national borders for years, but blockchain takes this globalization to another level. Parties conduct transactions and transfers between continents in a matter of minutes, and the digital infrastructure of the blockchain itself almost always transcends territorial boundaries. Adding to the difficulty, some of the largest cryptoasset exchanges operate outside of the United States, and many still require nothing more than an unverified email address before allowing an individual to begin trading. Finally, decentralized platforms, peer-to-peer exchangers, and anonymity-enhanced cryptocurrencies that use non-public or private blockchains all can further obscure financial transactions from legitimate scrutiny. As this Enforcement Framework makes clear, the challenges are significant. But so, too, are the resources that the U.S. Department of Justice, as well as the U.S. government as a whole, are dedicating to the effort, in collaboration with our international partners.

The Web 3.0

Technologists often talk about the Web 3.0, the next phase of the internet's evolution. On this vision, humans will reclaim the internet, their data, and their anonymity from large outside forces, whether they be corporate firms or government entities. Cryptocurrency—a medium of exchange defined, at its core, by a sense of private, individual control, and whose underlying blockchain technology already provides the backbone for applications outside the digital currency context—is central to this decentralized, anonymized, and still-being-defined notion of a future in which "a more semantically intelligent web" leverages data that "will be used by algorithms to improve user experience and make the web more personalized and familiar," and in which users will no longer have to "rely on network and cellular providers that surveil the information going through their systems."[viii] Ultimately, the Web 3.0 is a vision about the nature of data itself, foretelling a world in which information is diffuse and dynamic—present everywhere at once, and therefore beyond any outsider's grasp.

Only time will tell how, and in what form, the Web 3.0 finally takes shape. To its proponents, this vision marries technological innovation with human flourishing. This Enforcement Framework suggests that, however liberating the emerging glimpses of the Web 3.0 might seem to be, that vision also can pose uniquely dangerous threats to public safety. Confronting and addressing those threats is what good public policy should do—and what the crypto ecosystem itself may have to do, if its vision of the future is ever fully to take hold. Meanwhile, federal authorities will continue vigorously enforcing the law as it exists, and pursuing justice on behalf of the American people.

– **Sujit Raman**, *Chair,*
Attorney General's Cyber-Digital Task Force

Deputy Attorney General Jeffrey A. Rosen announces on September 22, 2020 the results of Operation DisrupTor, the U.S. government's largest operation to date targeting criminal activity on the darknet. The operation resulted in the arrest of nearly 180 dark web drug traffickers and criminals; the seizure of approximately 500 kilograms of illegal drugs worldwide; and the seizure of millions of dollars in cash and virtual currencies.

Cryptocurrency: An Enforcement Framework

Innovations in technology often change the world for the better. And yet, criminals, terrorists, and rogue states can use those same innovations for their own illegitimate ends, imposing great costs on the public. Today, few technologies are more potentially transformative and disruptive—and more potentially susceptible to abuse—than cryptocurrency.

Cryptocurrency is a form of virtual asset that uses cryptography to secure financial transactions. Many of cryptocurrency's central features—including decentralized operation and control, and, in some cases, a high degree of anonymity—present new and unique challenges for public safety that must be addressed, lest the technology be used predominantly for criminal activity. Indeed, despite its relatively brief existence, cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces. For example, cryptocurrency is increasingly used to buy and sell lethal drugs on the dark web (and by drug cartels seeking to launder their profits), contributing to a drug epidemic that killed over 67,000 Americans by overdose in 2018 alone.[1] Rogue states like Russia, Iran, and North Korea may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America's influence in the global marketplace. And, while terrorist use of cryptocurrency is still evolving, certain terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns.

The U.S. Department of Justice is responsible for investigating and prosecuting crimes and threats to national security, including those facilitated by the use of cryptocurrency. As consumers, investors, financial institutions, elected officials, and other stakeholders consider the future path of cryptocurrency and related technologies, we are publishing this Framework to enhance understanding of the associated public safety and national security challenges that these technologies present. These challenges impact the security and legitimacy of the cryptocurrency ecosystem itself; only by identifying and responsibly addressing them can the risks of cryptocurrency be mitigated. At a minimum, this means that entities that use or are impacted by cryptocurrency must understand their legal obligations and invest in meeting them. For example, cryptocurrency exchanges—including those physically located outside the United States—must take seriously their legal and regulatory obligations, discussed in greater detail below, to protect users and to safeguard potential evidence in criminal or national security investigations. Where a breach of these obligations might rise to the level of a criminal violation, the Department will take appropriate action.

In the pages that follow, we:

(1) describe how cryptocurrency technology is currently used and illustrate how malicious actors have misused that technology to harm cryptocurrency users, exchanges, and investors, as well as to facilitate a broad range of crimes from child exploitation to terrorism;

(2) identify some of the key legal authorities and partnerships the Department has relied upon to combat criminal and national security threats involving cryptocurrency; and

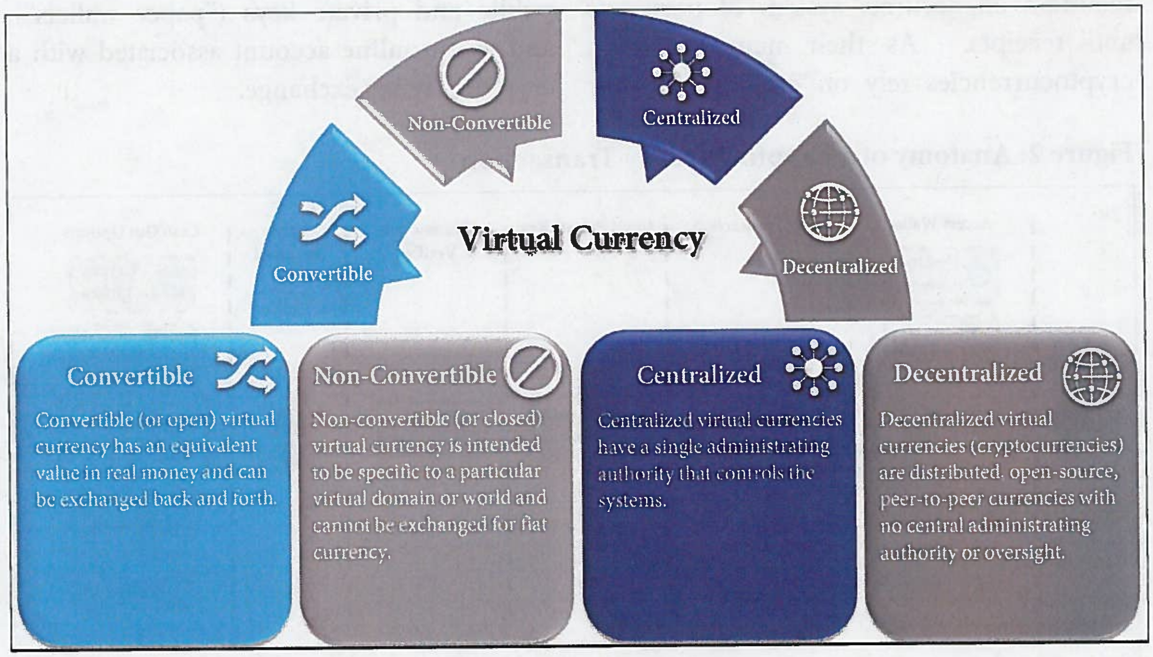
(3) discuss approaches for addressing the growing public safety challenges related to cryptocurrency.

I. Threat Overview

A. The Basics

"Virtual currency" is a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange—i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual currency is a type of "virtual asset" that is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets.[2] Moreover, unlike "traditional currency"—which is also referred to as fiat currency, real currency, or national currency—virtual currency does not have legal tender status in any particular country or for any government or other

Figure 1: Systemic Attributes of Virtual Currency



Convertible (or open) virtual currency has an equivalent value in real money and can be exchanged back and forth.

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world and cannot be exchanged for fiat currency.

Centralized virtual currencies have a single administrating authority that controls the systems.

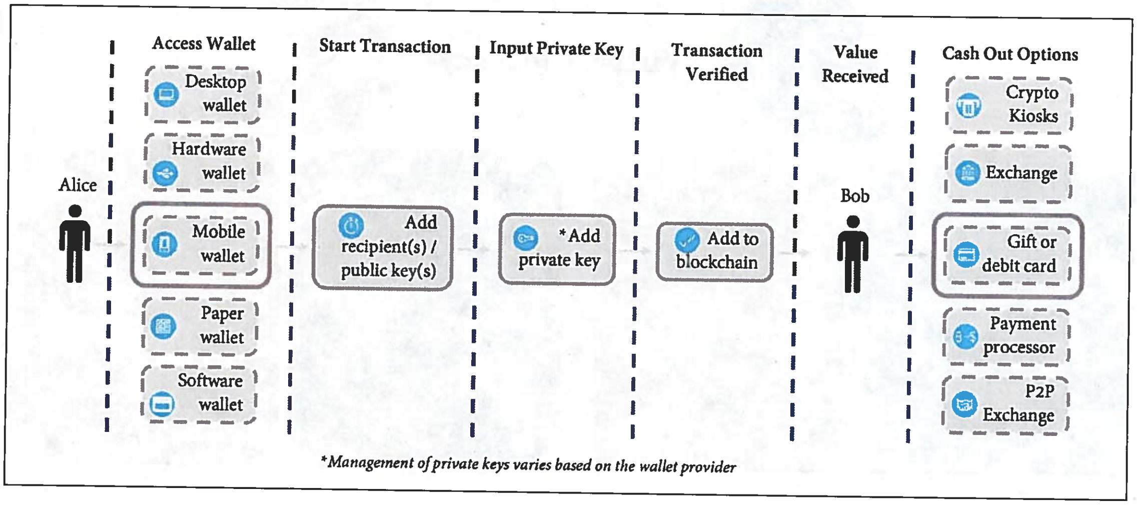
Decentralized virtual currencies (cryptocurrencies) are distributed, open-source, peer-to-peer currencies with no central administrating authority or oversight.

creditor.[3] Instead, the exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Virtual currency can be *convertible*, meaning it has an equivalent value in real currency or acts as a substitute for real currency, or *non-convertible*, meaning it is specific to a particular virtual domain—such as an online gaming community—and cannot be exchanged for real currency. [4]

"Cryptocurrency" refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, as they lack a central administrator to issue currency and maintain payment ledgers—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the "blockchain," and a network of peer-to-peer users to maintain an accurate system of payments and receipts. As their name suggests, cryptocurrencies rely on cryptography for security. Some examples of cryptocurrencies include Bitcoin,[5] Litecoin, and Ether.

Cryptocurrency can be exchanged directly person to person; through a cryptocurrency exchange; or through other intermediaries. The storage of cryptocurrency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the public keys (which are roughly akin to a bank account number) and private keys (which function like a PIN or password) that are used to send and receive cryptocurrency. Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device ("hardware wallets"); downloaded as software ("software wallets") onto either a personal computer or server ("desktop wallets") or an application on a smartphone ("mobile wallets"); as printed public and private keys ("paper wallets"); and as an online account associated with a cryptocurrency exchange.

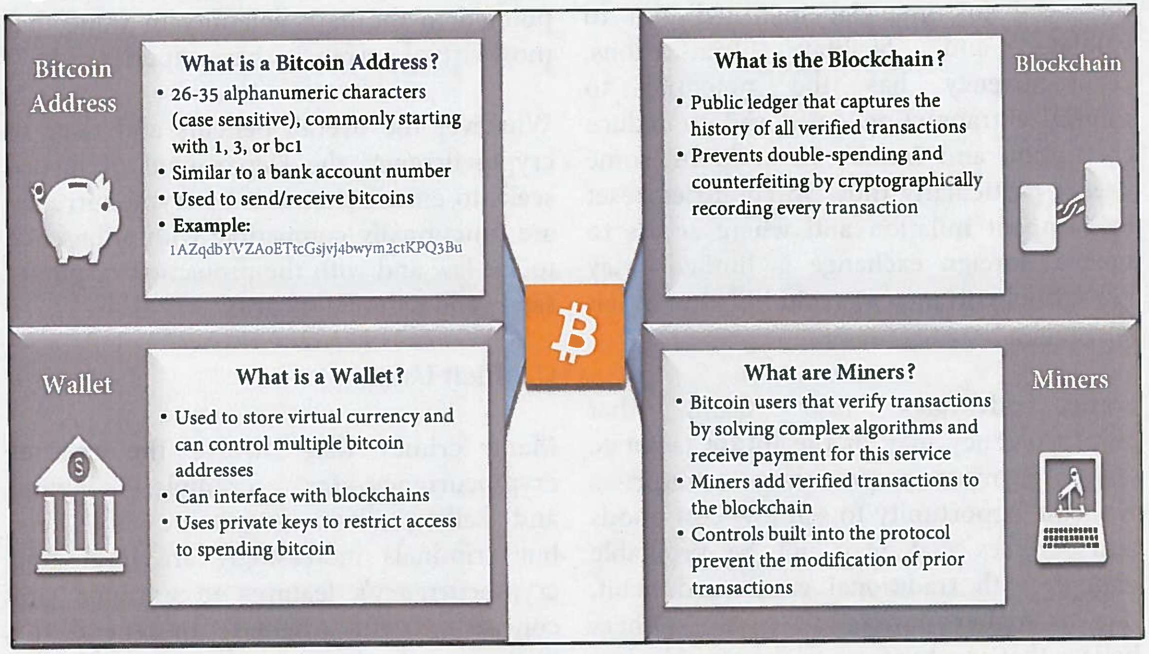
Figure 2: Anatomy of a Cryptocurrency Transaction



**Management of private keys varies based on the wallet provider*

The distributed ledger—which, as noted above, is known as the "blockchain" for most cryptocurrencies—allows such a decentralized system to accurately track payments and to prevent double-spending and counterfeiting by cryptographically recording every transaction. When a transaction is initiated, it is shared with participants on the network associated with the particular cryptocurrency, whereupon special users (often called "miners") verify that the units have not already been spent, and validate the transaction by solving a complex algorithm. The transaction is then added to the blockchain, with each block consisting of a group of reported transactions in chronological order. In exchange for participating in this community validation process, miners generate and receive a payment in the cryptocurrency itself—a process known as "mining."

Figure 3: Bitcoin Basics – Key Terms



Bitcoin Address

What is a Bitcoin Address?

- 26-35 alphanumeric characters (case sensitive), commonly starting with 1, 3, or bc1
- Similar to a bank account number
- Used to send/receive bitcoins
- **Example:** 1AZqdbYVZAoETtcGsjvj4bwym2ctKPQ3Bu

Blockchain

What is the Blockchain?

- Public ledger that captures the history of all verified transactions
- Prevents double-spending and counterfeiting by cryptographically recording every transaction

Wallet

What is a Wallet?

- Used to store virtual currency and can control multiple bitcoin addresses
- Can interface with blockchains
- Uses private keys to restrict access to spending bitcoin

Miners

What are Miners?

- Bitcoin users that verify transactions by solving complex algorithms and receive payment for this service
- Miners add verified transactions to the blockchain
- Controls built into the protocol prevent the modification of prior transactions

Cryptocurrencies can vary in their degree of anonymity depending on the public or non-public nature of their associated blockchain. For instance, while Bitcoin addresses do not have names or specific customer information attached to them, Bitcoin's blockchain is public. As a result, users can query addresses to view and understand Bitcoin transactions to some extent. Other cryptocurrencies, however, use non-public or private blockchains that make it more difficult to trace or to attribute transactions. These are often referred to as "anonymity enhanced cryptocurrencies" ("AECs") or "privacy coins." Examples of AECs include Monero, Zcash, and Dash.

B. Legitimate Uses

Cryptocurrency advocates maintain that a decentralized, distributed, and secure cryptocurrency holds great promise for legitimate use. Today's market includes over 2,000 cryptocurrencies, which enable users to transfer virtual currency around the globe in exchange for goods, services, and other sources of value. Proponents of cryptocurrency contend that, by eliminating the need for financial intermediaries to validate and facilitate transactions, cryptocurrency has the potential to minimize transaction costs and to reduce corruption and fraud. In addition, some users—particularly those in countries beset by rampant inflation and where access to normal foreign exchange is limited—may use virtual currency to avoid inflation in fiat currencies.

Some advocates also claim that cryptocurrency may in the future facilitate "micro-payments," providing enterprises with the opportunity to sell low-cost goods and services that may not be profitable enough with traditional credit and debit, due to higher transaction costs. Others believe that cryptocurrency can provide new access to markets, including to individuals in the developing world who are not served by banks or other financial institutions. Cryptocurrency advocates also stress that the privacy associated with cryptocurrency, though raising significant challenges for law enforcement, can have valid and beneficial uses. For example, such advocates claim that greater anonymity may reduce the risk of account or identity theft associated with the use of traditional credit systems.

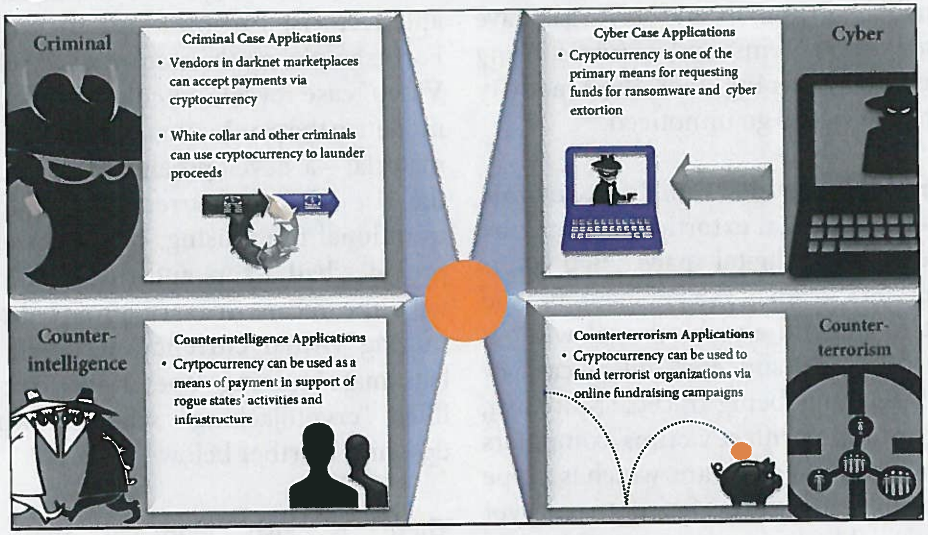
On the other hand, in addition to the substantial public safety and national security concerns discussed in this Framework, critics of cryptocurrency have raised questions about its supposed benefits. For example, certain critics contend that cryptocurrency could, if widely adopted, reduce the ability of national governments to regulate their economies through monetary policy. Others have raised concerns about the security of cryptocurrency wallets and exchanges, or pointed to the high volatility in value that most virtual currencies have experienced.

Whatever the overall benefits and risks of cryptocurrency, the Department of Justice seeks to ensure that uses of cryptocurrency are functionally compatible with adherence to the law and with the protection of public safety and national security.

C. Illicit Uses

Many crimes that involve the use of cryptocurrency—for example, buying and selling illicit drugs—are not new, but criminals increasingly are leveraging cryptocurrency's features to advance and conceal unlawful schemes. In general, the illicit use of cryptocurrency can fall into three broad categories. As explained further below, bad actors may exploit cryptocurrency to: (1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly

Figure 4 : Examples of Cryptocurrencies in Investigations



Criminal Case Applications

- Vendors in darknet marketplaces can accept payments via cryptocurrency
- White collar and other criminals can use cryptocurrency to launder proceeds

Cyber Case Applications

- Cryptocurrency is one of the primary means for requesting funds for ransomware and cyber extortion

Counterintelligence Applications

- Crytpocurrency can be used as a means of payment in support of rogue states' activities and infrastructure

Counterterrorism Applications

- Cryptocurrency can be used to fund terrorist organizations via online fundraising campaigns

implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.[6]

1. Using Cryptocurrency Directly to Commit Crimes or to Support Terrorism

Criminals use cryptocurrency to facilitate crimes and to avoid detection in ways that would be more difficult with fiat currency or "real money." They can avoid large cash transactions and mitigate the risk of bank accounts being traced, or of banks notifying governments of suspicious activity. Criminals have used cryptocurrency, often in large amounts and transferred across international borders, as a new means to fund criminal conduct ranging from child exploitation to terrorist fundraising. Cryptocurrency also has been used to pay for illegal drugs, firearms, and tools to commit cybercrimes, as well as to facilitate sophisticated ransomware and blackmail schemes.

Buying and selling illegal things. Criminals increasingly use cryptocurrency to purchase and to sell illicit items, such as drugs,[7] child sexual abuse material,[8] firearms, explosives, and toxic substances. There is also a robust market for counterfeit identification documents and for unlawfully obtained personal information, such as stolen credit card numbers. As discussed further below, purchases and sales of illegal goods and services using cryptocurrency often take place via dark web marketplaces created explicitly for the purpose of facilitating illicit transactions.[9]

Buying and selling tools to commit crimes or to support terrorism. Criminals and terrorists also use cryptocurrency to buy and sell "tools of the trade"—i.e., items that may or may not themselves be unlawful but are used for subsequent unlawful conduct. Such tools include raw materials to manufacture drugs or explosives, as well as cyber tools and computing capabilities (including servers and domains) to engage in cybercrime or to conduct malign influence campaigns over social media. Criminals and terrorists have purchased these items and services using cryptocurrency, hoping that their activity and planning would go unnoticed.[10]

Ransom, blackmail, and extortion. Increasingly, criminal extortion schemes are carried out in the digital space. Bad actors can use cryptocurrency as a payment method to facilitate ransom and blackmail without having to demand suitcases full of cash or risk bank accounts being traced. Moreover, criminals routinely infect victims' computers and servers with ransomware, which is a type of malicious software designed to encrypt or otherwise block access to valuable data until the victim agrees to provide a specified payment.[11] Criminals also demand payment after threatening to distribute confidential or embarrassing information (such as nude photos in cases of "sextortion") or engaging in "virtual kidnappings" where victims are misled into believing a loved one has been taken.

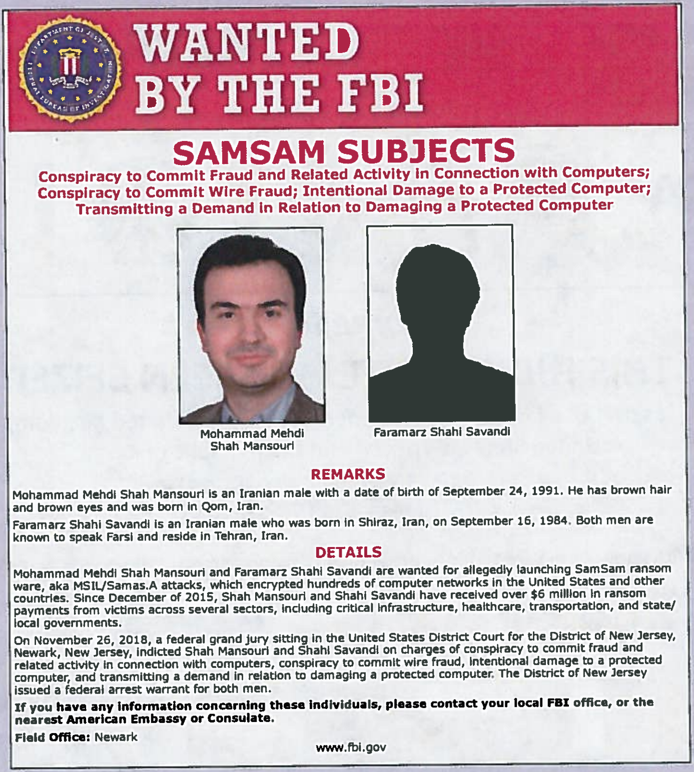
In April 2020, the Federal Bureau of Investigation ("FBI") issued an advisory about a potential increase in cryptocurrency fraud schemes due to the COVID-19 pandemic. The FBI noted that fraudsters were leveraging the fear and uncertainty caused by the pandemic to carry out scams in new ways. For example, some scammers threatened to infect victims and their families with coronavirus unless they sent payment in bitcoin. Others offered phony or defective products for sale using cryptocurrency with the promise that the products would cure or prevent the disease.[12]

Raising funds for criminal and terrorist activity. Cryptocurrency technology also has created new ways for criminal enterprises and terrorist organizations to raise funds. For example, as the notorious "Welcome to Video" case reveals, bitcoin has been used to monetize the production of child exploitation material—a development rarely seen before the rise of cryptocurrency. In addition to traditional fundraising, cryptocurrency also provides bad actors and rogue nation states with the means to earn profits directly by mining virtual currency, whether through legitimate mining operations or through illicit "cryptojacking" schemes, which are described further below.[13]

There is also evidence that certain terrorist groups are raising funds using cryptocurrency. While public data on terrorist use of cryptocurrency is limited, it is clear that terrorist networks have conducted fundraising operations through Internet-based crowdsource platforms in an attempt to evade stopgaps built into the international banking system.[14] In August 2015, for example, an individual was sentenced to over 11 years in federal prison for conspiring to provide material support and resources to the Islamic State of Iraq and al-Sham ("ISIS"), including by using social media to instruct donors on how bitcoin could provide untraceable financial support to terrorist groups.[15] More recently, in August 2020, the Department of Justice announced the government's largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and ISIS. Each of those groups had used cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns.[16]

SamSam

In a high-profile investigation into "21st-century digital blackmail," a federal grand jury in November 2018 indicted two Iranian men for a 34-month-long international computer hacking and extortion scheme involving the deployment of the sophisticated "SamSam" ransomware.[17] According to the indictment, starting in December 2015, the defendants allegedly accessed victims' computers, installed the SamSam ransomware, and then ran the program to encrypt critical data. The defendants demanded ransom paid in bitcoin in exchange for the keys needed to decrypt the victims' data. The defendants then allegedly exchanged the bitcoin proceeds into Iranian rial using Iran-based entities. All told, the defendants are alleged to have collected over $6 million in ransom payments and to have caused over $30 million in losses to more than 200 victims, which included hospitals, municipalities, and public institutions from around the world.



WANTED BY THE FBI

SAMSAM SUBJECTS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Mohammad Mehdi Shah Mansouri

Faramarz Shahi Savandi

REMARKS

Mohammad Mehdi Shah Mansouri is an Iranian male with a date of birth of September 24, 1991. He has brown hair and brown eyes and was born in Qom, Iran.

Faramarz Shahi Savandi is an Iranian male who was born in Shiraz, Iran, on September 16, 1984. Both men are known to speak Farsi and reside in Tehran, Iran.

DETAILS

Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi are wanted for allegedly launching SamSam ransom ware, aka MSIL/Samas.A attacks, which encrypted hundreds of computer networks in the United States and other countries. Since December of 2015, Shah Mansouri and Shahi Savandi have received over $6 million in ransom payments from victims across several sectors, including critical infrastructure, healthcare, transportation, and state/local governments.

On November 26, 2018, a federal grand jury sitting in the United States District Court for the District of New Jersey, Newark, New Jersey, indicted Shah Mansouri and Shahi Savandi on charges of conspiracy to commit fraud and related activity in connection with computers, conspiracy to commit wire fraud, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer. The District of New Jersey issued a federal arrest warrant for both men.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

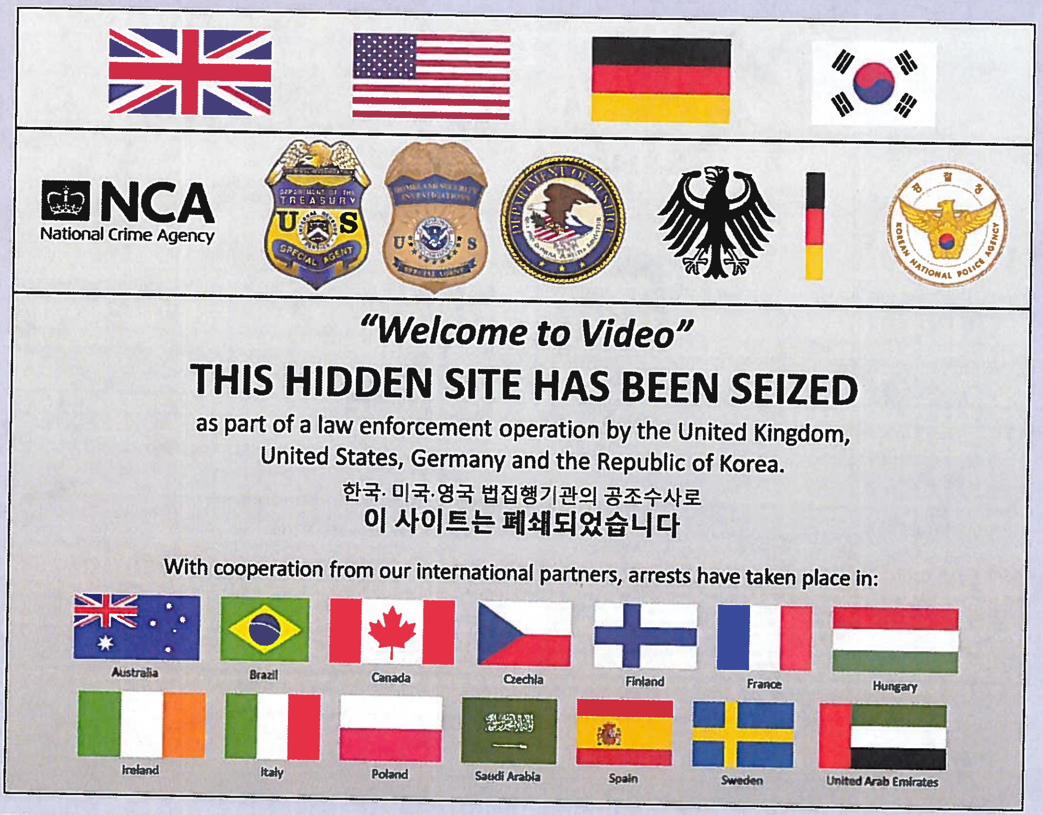
Field Office: Newark

www.fbi.gov

Figure 5: The "SamSam" Ransomware Attack – An Example of 21st Century Digital Blackmail

WELCOME TO VIDEO

On October 16, 2019, the Department of Justice announced the indictment and arrest of the alleged operator of Welcome to Video, a darknet child pornography website that was the world's largest online child sexual exploitation market at the time of its seizure. Welcome to Video allegedly offered child sexual exploitation photos and videos for sale using bitcoin, and relied on virtual currency accounts to fund the site and to promote further exploitation of children. The site allegedly hosted approximately eight terabytes of child sexual exploitation material—including over 250,000 unique videos—and claimed over one million downloads of exploitative material by its users. In addition to the operator, at least 337 users of the site have been arrested and charged across the United States and around the world. The globally coordinated law enforcement operation targeting Welcome to Video and its users led to the rescue of at least 23 minor victims who were actively being abused, allegedly by the site's users.[18]



"Welcome to Video"

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a law enforcement operation by the United Kingdom, United States, Germany and the Republic of Korea.

한국· 미국·영국 법집행기관의 공조수사로

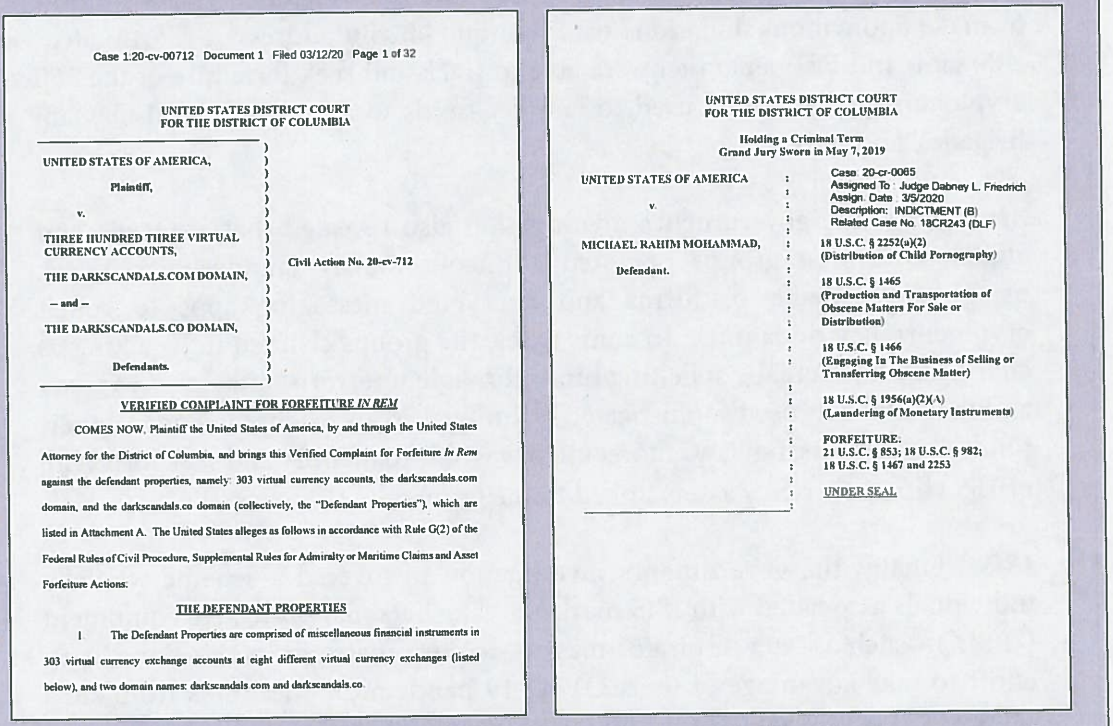
이 사이트는 폐쇄되었습니다

With cooperation from our international partners, arrests have taken place in:

Figure 6: Welcome to Video Website after Seizure by the Government

DarkScandals

A spin-off of the "Welcome to Video" investigation, the Department of Justice on March 12, 2020 announced the indictment of a Dutch national for his alleged operation of DarkScandals, a website that featured violent rape videos and depictions of child sexual abuse. According to the indictment, DarkScandals hosted over 2,000 videos and images advertised as including "real blackmail, rape and forced videos of girls all around the world."[19] Users could allegedly access the illicit content by paying cryptocurrency or by uploading new content depicting rape or other sexual abuse. The site's alleged operator was charged with distribution of child pornography; production and transportation of obscene matters for sale or distribution; engaging in the business of selling or transferring obscene matter; and money laundering. In addition, the government filed a civil forfeiture action seeking recovery of illicit funds from 303 virtual currency accounts allegedly used by customers to fund DarkScandals and to promote child exploitation.[20]



Case 1:20-cv-00712 Document 1 Filed 03/12/20 Page 1 of 32

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. THREE HUNDRED THREE VIRTUAL CURRENCY ACCOUNTS, THE DARKSCANDALS.COM DOMAIN, — and — THE DARKSCANDALS.CO DOMAIN, Defendants.	Civil Action No. 20-cv-712

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America, by and through the United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture *In Rem* against the defendant properties, namely: 303 virtual currency accounts, the darkscandals.com domain, and the darkscandals.co domain (collectively, the "Defendant Properties"), which are listed in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions:

THE DEFENDANT PROPERTIES

1. The Defendant Properties are comprised of miscellaneous financial instruments in 303 virtual currency exchange accounts at eight different virtual currency exchanges (listed below), and two domain names: darkscandals.com and darkscandals.co.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in May 7, 2019

UNITED STATES OF AMERICA v. MICHAEL RAHIM MOHAMMAD, Defendant.	Case: 20-cr-0065 Assigned To : Judge Dabney L. Friedrich Assign. Date : 3/5/2020 Description: INDICTMENT (B) Related Case No. 18CR243 (DLF) 18 U.S.C. § 2252(a)(2) (Distribution of Child Pornography) 18 U.S.C. § 1465 (Production and Transportation of Obscene Matters For Sale or Distribution) 18 U.S.C. § 1466 (Engaging In The Business of Selling or Transferring Obscene Matter) 18 U.S.C. § 1956(a)(2)(A) (Laundering of Monetary Instruments) FORFEITURE: 21 U.S.C. § 853; 18 U.S.C. § 982; 18 U.S.C. § 1467 and 2253 UNDER SEAL

Figure 7: The Indictment and Civil Forfeiture Papers Filed by the Government in the DarkScandals Matter

DISMANTLING OF TERRORIST FINANCING CAMPAIGNS

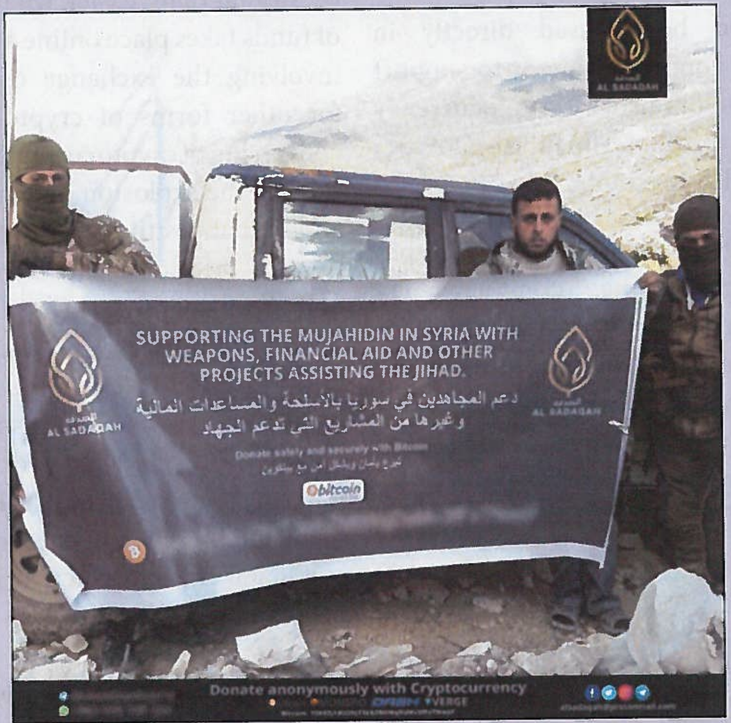
On August 13, 2020, the Department of Justice announced the dismantling of three terrorist financing cyber-enabled campaigns involving the al-Qassam Brigades, al-Qaeda, and ISIS. Investigation revealed that these terrorist groups used sophisticated cyber-tools to assist in financing their operations, including through online solicitation of cryptocurrency donations from supporters around the world. The government has filed three civil forfeiture complaints and a criminal complaint involving the seizure of four websites, four Facebook pages, over 300 cryptocurrency accounts, and millions of dollars.

Al-Qassam Brigades. According to the government's complaint, the al-Qassam Brigades posted requests for bitcoin donations on its social media page and official websites, claiming that such donations would be untraceable and used to support violent causes. The group's websites included videos on how to make anonymous donations using unique bitcoin addresses. Fortunately, IRS, HSI, and FBI personnel were able to track and seek forfeiture of the 150 cryptocurrency accounts used to launder funds to and from the al-Qassam Brigades' accounts.

Al-Qaeda. The government's investigation also revealed that al-Qaeda and affiliated terrorist groups operated a bitcoin money laundering network using social media platforms and encrypted messaging apps to solicit cryptocurrency donations. In some cases, the groups claimed to be acting as charities, while actually soliciting funds for violent terrorist attacks. Al-Qaeda and their affiliates used sophisticated techniques in an attempt to conceal their fundraising efforts, but law enforcement was able to identify and seek forfeiture of 155 virtual currency assets linked to the groups.

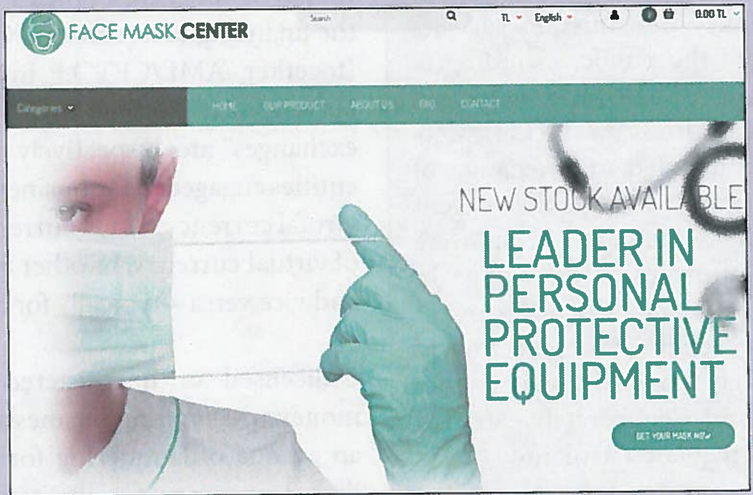
ISIS. Finally, the government's investigation uncovered a scheme whereby individuals associated with ISIS marketed fake personal protective equipment ("PPE")—such as N95 respirator masks—to customers across the globe in an effort to take advantage of the COVID-19 pandemic. The funds from such sales would have been used to support ISIS's operations.[21]

Figure 8: "*Donate Anonymously with Cryptocurrency*" – An al-Qaeda-Affiliated Group Seeks Anonymous Donations in Bitcoin


AL SADAQAH
SUPPORTING THE MUJAHIDIN IN SYRIA WITH WEAPONS, FINANCIAL AID AND OTHER PROJECTS ASSISTING THE JIHAD.
دعم المجاهدين في سوريا بالأسلحة والمساعدات المالية
وغيرها من المشاريع التي تدعم الجهاد
Donate safely and securely with Bitcoin
bitcoin
Donate anonymously with Cryptocurrency

The group that posted the request for donations claimed to be a Syrian charity, but allegedly sought funds to support "the mujahidin in Syria with weapons, financial aid and other projects assisting the jihad." [22]

Figure 9: Website Maintained by an ISIS Facilitator to Sell Fake PPE



2. Using Cryptocurrency to Hide Financial Activity

In addition to being used directly in transactions to commit crime or to support terrorism, bad actors also use cryptocurrency to hide and to promote financial activities attendant to unlawful conduct.

Money laundering. Criminals of all types are increasingly using cryptocurrency to launder their illicit proceeds. Broadly speaking, money laundering occurs when an individual knowingly conducts a financial transaction connected to or stemming from a criminal offense in order to promote the offense, conceal the proceeds, or evade federal reporting requirements.[24] Such conduct can be substantially easier when the movement of funds takes place online and anonymously, involving the exchange of cryptocurrency for other forms of cryptocurrency or the conversion of cryptocurrency to fiat currency. Indeed, the explosion of online marketplaces and exchanges that use cryptocurrency may provide criminals and terrorists with new opportunities to transfer illicitly obtained money in an effort to cover their financial footprints and to enjoy the benefits of their illegitimate earnings. Transnational criminal organizations, including drug cartels, may find cryptocurrency especially useful to hide financial activities and to move vast sums of money efficiently across borders without detection.

BITCOIN MAVEN

In July 2018, Theresa Tetley, known by her online moniker "Bitcoin Maven," was sentenced to one year in federal prison for money laundering and for operating an unlicensed bitcoin-for-cash money-transmitting business. Through her unregistered bitcoin exchange business, Tetley facilitated money laundering by providing money-transmission services to members of the public, including at least one individual who received bitcoin from the sale of drugs on the dark web. Tetley also conducted an exchange of bitcoin for cash with an undercover agent who represented that his bitcoin were the proceeds of narcotics trafficking. In sentencing documents, the government revealed that Tetley's business "fueled a black-market financial system" that "purposely and deliberately existed outside of the regulated bank industry."[23]

Operating unlicensed, unregistered, or non-compliant exchanges. Criminals may also attempt to hide financial activity by using cryptocurrency exchanges that do not comply with internationally recognized anti-money laundering ("AML") and combating the financing of terrorism ("CFT") standards (together, "AML/CFT").[25] In general, "virtual currency exchangers" and "virtual currency exchanges" are, respectively, individuals and entities engaged in the business of exchanging virtual currency for fiat currency, other forms of virtual currency, or other types of assets—and vice versa—typically for a commission.[26]

Unlicensed or unregistered exchanges or money transmitting businesses can "provide an avenue of laundering for those who use digital currency for illicit purposes."[27] In addition, even properly registered exchanges can serve as a haven for criminal activity by operating under lax rules or by flouting AML protocols. In the normal course, registered exchanges that comply with AML standards and "know your customer" ("KYC") requirements are likely to possess relevant transactional information. However, exchanges that avoid compliance with such requirements provide criminals and terrorists with opportunities to hide their illicit financial activity from regulators and investigators. Moreover, as discussed in Part II.C below, the requirements for exchanges to register, obtain licenses, and collect information about customers and their transactions are not consistent across international jurisdictions. This inconsistency can create challenges for international law enforcement and regulatory agencies operating in this space.

Evading taxes. As with money laundering, the potential difficulties in tracking cryptocurrency transactions can also facilitate tax evasion. Because of these difficulties, tax cheats may believe that the Internal Revenue Service is not able to uncover or attribute their cryptocurrency transactions, and they may even use additional anonymizing features of cryptocurrencies to further obfuscate their transactions. Tax cheats may then attempt tax evasion by, among other things, not reporting capital gains from the sale or other disposition of their cryptocurrency, not reporting business income received in cryptocurrency, not reporting wages paid in cryptocurrency, or using cryptocurrency to facilitate false invoice schemes designed to fraudulently reduce business income.[30] Importantly, the tax loss from unreported capital gains can

BTC-e

In 2017, prosecutors in the United States announced the indictment of the virtual currency exchange "BTC-e" and of one of the exchange's principal operators. BTC-e received more than $4 billion worth of bitcoin over the course of its operation. According to the indictment, to appeal to criminals as a customer base, BTC-e did not require users to validate their identities, obscured and anonymized transactions and sources of funds, and lacked appropriate anti-money laundering processes. As a result, the exchange predictably served as a hub for international criminals seeking to hide and launder ill-gotten gains. The indictment alleges that BTC-e facilitated transactions for cybercriminals worldwide and received criminal proceeds from numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. The Department of Justice filed criminal charges, and the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") assessed a $110 million civil penalty against the exchange for willfully violating U.S. anti-money laundering laws, and a $12 million penalty against the exchange's operator personally.[28] BTC-e is only one example in a series of cases in which the Department of Justice has pursued criminal charges against cryptocurrency exchanges for operating as unlicensed money services businesses.[29]

be significant as cryptocurrencies emerge and fluctuate in the market. For example, the value of one bitcoin famously rose from around $1,000 to around $20,000 in 2017, as investors rushed to that cryptocurrency as an investment vehicle.

Avoiding sanctions. Finally, individuals, companies, and rogue regimes may use cryptocurrency in attempt to avoid the reach of economic sanctions imposed by the United States or other rule-of-law countries. Cryptocurrency's decentralized and peer-to-peer format may allow sanctioned entities to bypass the financial controls built into traditional financial marketplaces to enforce such sanctions. Indeed, public reports note that several nations have explored the creation and use of their own state-sponsored cryptocurrencies, which could serve as a platform to evade financial controls and oversight. As explained by the U.S. Department of the Treasury, for example, Venezuela attempted to launch a national cryptocurrency—called the "Petromoneda" or "Petro"—in the "hope that the [cryptocurrency] would allow Venezuela to circumvent U.S. financial sanctions."[31] Other countries, including Russia and Iran, have threatened to use existing cryptocurrencies to dodge sanctions or to develop their own cryptocurrencies specifically to avoid international oversight.[32]

3. Committing Crimes within the Cryptocurrency Marketplace Itself

In addition to offering a means to commit old crimes in new ways, cryptocurrencies and the platforms on which they operate have often themselves become the target of criminal activity. To protect future victims, as well as to safeguard the integrity of cryptocurrency technology, more must be done to promote security and combat criminal activity on digital exchanges and platforms.

Theft and fraud. Cryptocurrency's features, as well as the overall "opaqueness and lack of transparency in the cryptocurrency market,"[33] make it particularly attractive, adaptable, and scalable as a target for theft. Criminals—and even rogue state actors[34]—can steal cryptocurrency by exploiting security vulnerabilities in wallets and exchanges. Thieves can hack wallets and exchanges directly; employ social engineering and other tools to obtain passwords and PINs from unsuspecting users; or, if they themselves operate exchanges, engage in insider theft. Public reports estimate that at least $1.7 billion of cryptocurrency was stolen or scammed in 2018, with over $950 million of that amount stolen from cryptocurrency exchanges. In 2019, over $4.5 billion of cryptocurrency reportedly was lost to theft or fraud, more than doubling the losses from the prior year.[35] This susceptibility to theft on a massive scale demonstrates that the lack of appropriate regulation and monitoring of cryptocurrency exchanges poses a threat to cryptocurrency users themselves, as well as to the general public.

In addition to digital theft, fraudsters use cryptocurrency to bilk unsuspecting investors, to promote scams, and to engage in market manipulation. For example, in July 2018, Jon E. Montroll pleaded guilty to securities fraud and to obstruction of justice related to his operation of two online Bitcoin services: WeExchange Australia, Pty. Ltd., a Bitcoin depository and currency exchange service, and BitFunder.com, which facilitated the purchase and trading of virtual shares of business entities that listed shares on the platform. Montroll pleaded guilty to converting a portion of WeExchange users' bitcoin to his personal use without the users' knowledge or consent. Montroll also admitted failing to disclose a hack of the BitFunder programming code that caused the platform to credit hackers with profits they did not earn, thereby enabling the hackers to wrongfully withdraw approximately 6,000 bitcoin. The hack meant that Montroll lacked the bitcoin necessary to cover what he owed to investors. Despite this, and as a result of his omissions and misrepresentations, Montroll still raised approximately 978 bitcoin after the discovery of the hack. In addition to committing securities fraud, Montroll provided a falsified screenshot and false and misleading answers to Securities and Exchange Commission ("SEC") personnel during the course of their investigation.[36]

In another fraudulent scheme involving cryptocurrency, Joseph Kim was sentenced in November 2018 to 15 months in federal prison for misappropriating $1.1 million in bitcoin and litecoin. Kim worked as an assistant trader for a Chicago trading firm that had formed a cryptocurrency group to engage in trading of virtual currencies. Over a two-month period in 2017, Kim misappropriated at least $600,000 of his trading firm's bitcoin and litecoin cryptocurrency for his own personal benefit, and made false statements and representations to the company's management to conceal the theft. Subsequently, Kim engaged in another scheme in which he incurred $545,000 in losses by trading cryptocurrencies using funds that he solicited from friends through lies.[37]

Cryptojacking. The ability to digitally mine cryptocurrency provides criminals an independent reason to hack into and co-opt computers belonging to unsuspecting individuals and organizations. The unauthorized use of someone else's computer to generate (or "mine") cryptocurrency is called "cryptojacking."[38] This is often accomplished through the use of malware or compromised websites, which cause the victim's computer to run crypto-mining code. Considering the value of cryptocurrency compared to the relative ease of secretly using a victim's computer, cryptojacking is another relatively low-risk but high-reward illegal activity made possible by cryptocurrency technology. Reports indicate that rogue states, such as North Korea, have explored using malware to mine cryptocurrency illicitly.[39]

D. The Role of Darknet Markets

Many of the cryptocurrency-related crimes described above are made possible through the operation of online black markets on the dark web. Indeed, much of the illicit conduct involving cryptocurrency occurs via darknet websites and marketplaces that allow criminals around the world to connect in unregulated virtual bazaars with a great deal of anonymity. These illicit marketplaces offer the opportunity not only to buy and to

Operation DisrupTor

In September 2020, the Department of Justice joined Europol to announce the results of Operation DisrupTor, a coordinated international effort to disrupt opioid trafficking on the dark web. The extensive operation lasted nine months and was conducted across the United States and Europe, demonstrating international law enforcement's continued partnership against the illegal sale of drugs and other illicit goods and services.

Following the Wall Street Market takedown in May 2019, U.S. and international law enforcement agencies obtained intelligence to identify dark web drug traffickers, resulting in a series of complementary, but separate, law enforcement investigations. Operation DisrupTor actions have resulted in the arrest of 179 dark web drug traffickers and fraudulent criminals who engaged in tens of thousands of sales of illicit goods and services across the United States and Europe.

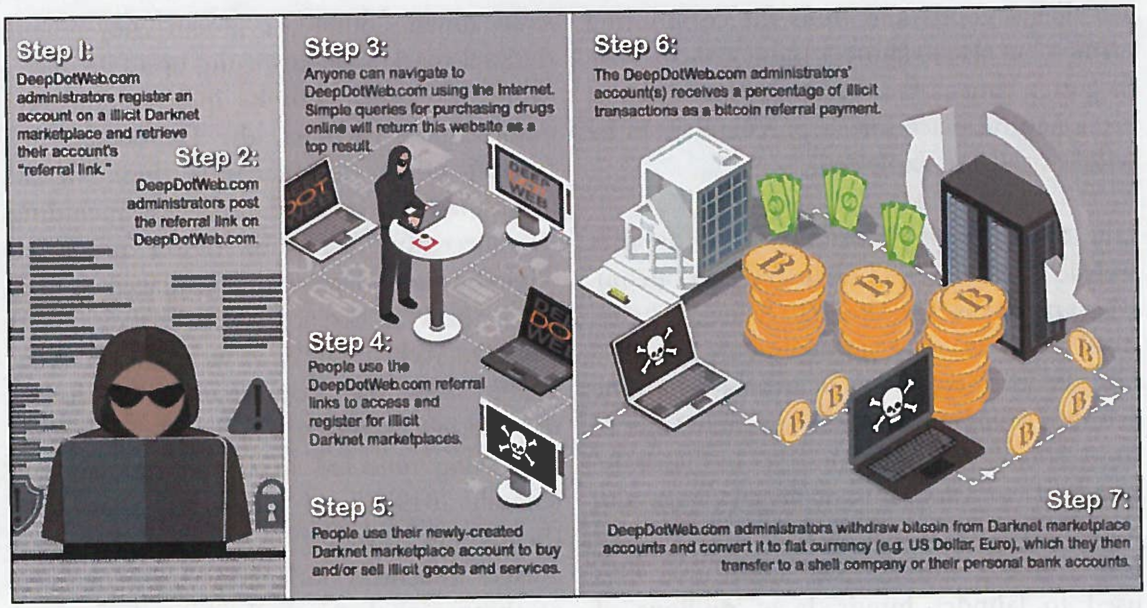
This operation resulted in the seizure of over $6.5 million in both cash and virtual currencies; approximately 500 kilograms of drugs worldwide; 274 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances in the United States; and 63 firearms.

Operation DisrupTor led to 121 arrests in the United States including two in Canada at the request of the United States, 42 in Germany, eight in the Netherlands, four in the United Kingdom, three in Austria, and one in Sweden. A number of investigations are still ongoing to identify the individuals behind dark web accounts. Operation DisrupTor illustrates the investigative power of federal and international partnerships to combat the borderless nature of online criminal activity, including activity using cryptocurrency.

U.S. Immigration and Customs Enforcement
EUROPOL
EUROJUST
Operation DisrupTor
85
Darknet drug traffickers arrested in US
Over $6.5 million
in both cash and virtual currencies seized
Over 270
kilograms of drugs seized
63
firearms seized
179 Total Arrests Worldwide

DeepDotWeb

In May 2019, the Department announced the indictment of the alleged owners and operators of the website known as DeepDotWeb ("DDW") on charges of money laundering conspiracy. According to the indictment, DDW served as a gateway that provided users with access to numerous darknet marketplaces offering for sale illegal narcotics (including fentanyl, heroin, and crystal meth), firearms, malicious software, hacking tools, stolen credit card information, and other contraband. The owners of DDW allegedly received payments—styled as "referral bonuses"—paid in virtual currency to a DDW-controlled bitcoin wallet from individuals who used the site to purchase illicit items. DDW's owners allegedly attempted to conceal the nature of these illegal payments, which totaled more than $15 million, by transferring the bitcoin they received to other bitcoin addresses and to bank accounts opened under the names of shell companies. During the course of the conspiracy, DDW's owners are alleged to have referred hundreds of thousands of users to darknet marketplaces, including AlphaBay, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D's, Wall Street Market, and Tochka Market. In turn, these users completed hundreds of millions of dollars' worth of allegedly illicit transactions.[40]



Step l:
DeepDotWeb.com administrators register an account on a illicit Darknet marketplace and retrieve their account's "referral link."

Step 2:
DeepDotWeb.com administrators post the referral link on DeepDotWeb.com.

Step 3:
Anyone can navigate to DeepDotWeb.com using the Internet. Simple queries for purchasing drugs online will return this website as a top result.

Step 4:
People use the DeepDotWeb.com referral links to access and register for illicit Darknet marketplaces.

Step 5:
People use their newly-created Darknet marketplace account to buy and/or sell illicit goods and services.

Step 6:
The DeepDotWeb.com administrators' account(s) receives a percentage of illicit transactions as a bitcoin referral payment.

Step 7:
DeepDotWeb.com administrators withdraw bitcoin from Darknet marketplace accounts and convert it to fiat currency (e.g. US Dollar, Euro), which they then transfer to a shell company or their personal bank accounts.

Figure 10: Anatomy of the DeepDotWeb Criminal Operation

DREAM MARKET

In October 2018, an administrator of the darknet marketplace Dream Market was sentenced to 20 years in federal prison for narcotics trafficking and money laundering. The defendant, Gal Vallerius, initially participated in the marketplace as a vendor, selling Oxycodone and Ritalin. He later acted as an administrator and senior moderator, supporting illicit narcotics and money laundering transactions between the site's buyers and vendors. Following the dismantling of Silk Road and AlphaBay, Dream Market had become one of the largest darknet criminal marketplaces, and all of its items and services were offered for sale in exchange for bitcoin or other peer-to-peer cryptocurrencies.

sell illegal goods and tools for committing crimes, but also to launder money and to hide ill-gotten gains. As a result, darknet markets are a natural place for cryptocurrency to be widely used and exploited.

One of the most notorious online darknet websites, which relied exclusively on bitcoin, was known as Silk Road. Prior to being dismantled by law enforcement in 2013, Silk Road served as an extensive online criminal marketplace used by thousands of drug dealers and other vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers. Silk Road was also used to launder hundreds of millions of dollars in illicit proceeds. When the site was shut down, other cryptocurrency-reliant darknet marketplaces sprung up in its place. Working closely with its international law enforcement partners, the Department of Justice's efforts to dismantle these virtual black markets continue in earnest, including the successful disruption of the notorious AlphaBay and Hansa marketplaces in July 2017; the Wall Street Market ("WSM") and DeepDotWeb ("DDW") websites in May 2019;[41] and the coordinated takedowns of darknet markets dedicated to opioid trafficking reflected in Operation SaboTor (March 2019)[42] and Operation DisrupTor (September 2020).[43] Cryptocurrencies played a central facilitating role in each of these global criminal enterprises. For example, as the Department announced at the time that indictments were returned against the alleged owners and operators of DDW, "Between in and around November 2014 and April 10, 2019, DDW received approximately 8,155 bitcoin in kickback payments from darknet marketplaces, worth approximately $8,414,173 when adjusted for the trading value of bitcoin at the time of each transaction."[44] Attesting to the complexity of these illicit cross-border payments, many of which took place entirely outside of the established international banking network, the bitcoin was transferred to DDW's bitcoin wallet, which the defendants are alleged to have controlled, in a series of "more than 40,000 deposits," and was subsequently withdrawn to various destinations (both known and unknown) around the world through over 2,700 transactions.[45]

II. Law and Regulations

As discussed in Part I, a wide range of criminal activity may involve or be facilitated by the use of cryptocurrency. On numerous occasions, the Department of Justice has used available legal tools to pursue successful prosecutions of such activity. This Part provides an overview of the legal authorities the Department uses to prosecute those who misuse cryptocurrency, and describes the roles and responsibilities of the Department's key government partners.

A. Criminal Code Authorities

As discussed above, cryptocurrency is often the preferred payment method for the distribution of contraband and of other illegal goods and services, and it can be used to collect funds from victims of traditional fraud or computer intrusions. A wide variety of federal charges can be brought to bear for such conduct, including, for example:

- **Wire fraud,** 18 U.S.C. § 1343. (For examples of cryptocurrency prosecutions involving the wire fraud statute, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)

- **Mail fraud,** 18 U.S.C. § 1341.

- **Securities fraud,** 15 U.S.C. §§ 78j and 78ff. (For example, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of Jon E. Montroll, discussed on pages 15-16.)

- **Access device fraud,** 18 U.S.C. § 1029. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

- **Identity theft and fraud,** 18 U.S.C. § 1028. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

- **Fraud and intrusions in connection with computers,** 18 U.S.C. § 1030. (For example, see the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)

- **Illegal sale and possession of firearms,** 18 U.S.C. § 921 *et seq.*

- **Possession and distribution of counterfeit items,** 18 U.S.C. § 2320.

- **Child exploitation activities,** 18 U.S.C. § 2251 *et seq.* (For example, see the indictment of Ammar Atef Alahdali, discussed on page 6, footnote 8.)

- **Possession and distribution of controlled substances,** 21 U.S.C. § 841 *et seq.* (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

The Department also can bring to bear a wide variety of money laundering charges in cases involving misuse of cryptocurrency. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering violations. In addition, individuals and companies engaged in money transmission involving virtual assets, referred to below as "virtual asset service providers," may be subject to, and may fail to comply with, both federal and State registration, record keeping, and reporting requirements. Potential charges include, for example:

- **Money laundering,** 18 U.S.C. § 1956 *et seq.* (For examples of cryptocurrency prosecutions involving the federal money laundering statute, see the indictment of BTC-e and its operator, discussed on pages 14 and 46; the indictment of AlphaBay, discussed on pages 19 and 47; the indictment of a Dutch national for his operation of DarkScandals, discussed on page 10; and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Transactions involving proceeds of illegal activity,** 18 U.S.C. § 1957. (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46.)

- **Operation of an unlicensed money transmitting business,** 18 U.S.C. § 1960 (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46, and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Failure to comply with Bank Secrecy Act requirements,** 31 U.S.C. § 5331 *et seq.*

Virtual asset transactions may also form the basis for prosecution if, for example, they are used as a means to provide material support or resources to terrorists or foreign terrorist organizations.[46] Such transactions could also be used for payments that facilitate other crimes implicating national security, such as espionage[47] or conspiracies involving interference in the political process, in violation of various federal laws.

Finally, the Department frequently uses existing criminal authorities to seize and forfeit virtual assets and other property derived from or involved in activity of an individual or organization charged with a crime. The Department also uses available civil authorities for such seizures and forfeitures, which allow the government to "arrest" the assets themselves, even in cases where no person is charged criminally or where a defendant may not be prosecutable due to, for example, death or flight from a jurisdiction. Statutory authorities for forfeiture include:

- **Criminal forfeiture,** 18 U.S.C. § 982; 21 U.S.C. § 853. (For examples of cryptocurrency prosecutions involving the criminal forfeiture statute, see the indictment of the alleged administrator of Helix, discussed on page 43, and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Civil forfeiture,** 18 U.S.C. § 981. (For example, see the verified complaints in the AlphaBay case, discussed on pages 9 and 47; the Welcome to Video case, discussed on pages 7 and 9; the DarkScandals case, discussed on page 10; the cases involving the al-Qassam Brigades, al-Qaeda, and ISIS, discussed on pages 7 and 11-12; and the cases involving hacks of virtual currency exchanges by North Korean actors, discussed on pages 27 and 28.)

B. Regulatory Authorities

As described above, the Department of Justice has broad and diverse federal jurisdiction over criminal and other improper conduct that may involve cryptocurrency and other types of virtual assets. A number of regulatory agencies in the United States also have authority to enforce statutes and regulations that apply to various virtual-asset-related activities. The Department has worked closely and cooperatively with these agencies in identifying and proceeding against individuals who misuse cryptocurrency for illicit purposes.

Much of the regulatory activity conducted by the agencies discussed below focuses on money services businesses ("MSBs") and virtual asset service providers ("VASPs"). In general, MSBs are individuals or entities in one or more of the following capacities:

i. currency dealer or exchanger;

ii. check casher;

iii. issuer of traveler's checks, money orders, or stored value;

iv. seller or redeemer of traveler's checks, money orders, or stored value;

v. money transmitter; or

vi. the U.S. Postal Service.[48]

VASPs are individuals or entities operating as a business to conduct one or more of the following activities for or on behalf of another entity or individual:

i. exchanges between virtual assets and fiat currencies;

ii. exchanges between one or more forms of virtual assets;

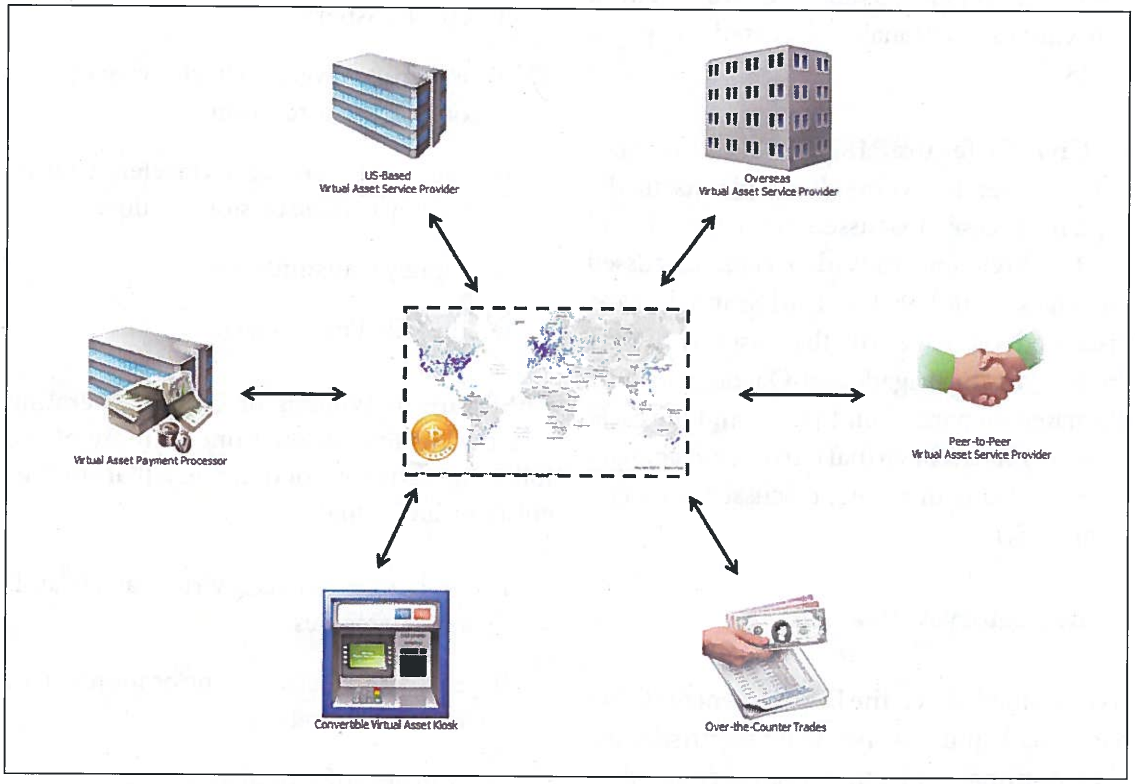
iii. transfers of virtual assets;

iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or

v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[49]

In the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs. Like brick-and-mortar financial institutions, MSBs are subject to AML/CFT[50] regulations as well as certain licensing and registration requirements, as discussed below.

Figure 11: Depiction of the Operation of a Global Virtual Asset Network


US-Based
Virtual Asset Service Provider
Overseas
Virtual Asset Service Provider
Virtual Asset Payment Processor
Peer-to-Peer
Virtual Asset Service Provider
Convertible Virtual Asset Kiosk
Over-the-Counter Trades

1. The Financial Crimes Enforcement Network and the Bank Secrecy Act

Regulatory authority. MSBs, including cryptocurrency exchanges, function as regulated businesses subject to the federal Bank Secrecy Act ("BSA").[51] The U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") has primary responsibility for administering the BSA and for implementing its regulations.[52] Part of that responsibility includes maintaining the BSA database, which is a repository of reports about financial transactions that are potentially indicative of money laundering.[53] FinCEN serves as the Financial Intelligence Unit ("FIU") for the United States, meaning it is the central entity responsible for receiving and analyzing suspicious transaction reports and other information concerning money laundering, financing of terrorism, and related offenses.[54] FinCEN regulates individuals and entities engaged in the business of accepting and transmitting convertible virtual currency ("CVC"), which refers to "virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of 'value that substitutes for currency.'"[55] In 2011, FinCEN issued a final rule that, among other things, defined "money transmission services" to include accepting and transmitting "currency, funds, or *other value that substitutes for currency* by any means."[56] The phrase "other value that substitutes for currency" was intended to cover situations where a transmission includes something that the parties recognize has value that is equivalent to, or can substitute for, fiat currency.[57] The definition of "money transmission" is technology-neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another, or from one location to another, is regulated under the BSA.

To provide additional clarity and to respond to questions from the private sector, FinCEN issued interpretive guidance in March 2013 and in May 2019 regarding the application of its regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency.[58] The 2013 FinCEN guidance identified the participants in some virtual currency arrangements, including "exchangers," "administrators," and "users," and clarified that while exchangers and administrators generally qualify as money transmitters under the BSA, users do not.[59] The guidance also stated that virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered MSBs to the extent they accept and transmit CVC or when they buy or sell CVC for any reason.[60] As MSBs, such virtual currency administrators and exchangers are obliged to have AML programs, to file Suspicious Activity Reports ("SARs"), and to follow other BSA requirements.[61]

The May 2019 FinCEN guidance addressed how FinCEN regulations relating to MSBs apply to various business models involving money transmission denominated in CVC, including with reference to prior administrative rulings.[62] Importantly, the guidance discussed the application of the BSA to foreign-located MSBs, individual peer-to-peer exchangers, wallet providers, cryptocurrency kiosk operators, CVC-to-CVC transactions, payment processors, mixers and tumblers, initial coin offerings, Internet casinos, trading platforms, decentralized exchanges and distributed applications ("DApps"), miners, software providers, and developers of such technologies. In particular, the guidance outlined the application of FinCEN's regulations to persons who provide anonymizing services or who are engaged in activities involving anonymity-enhanced CVCs. According to FinCEN, anonymizing service providers and some AEC issuers are money transmitters, whereas an individual or entity that merely provides anonymizing software is not.

FinCEN has stated that MSBs that conduct money transmission in CVCs must meet the same AML/CFT standards as other MSBs under the Bank Secrecy Act. This includes registering with FinCEN, establishing an AML program reasonably designed to prevent money laundering and terrorist financing, and meeting certain record keeping and reporting obligations, such as filing SARs.[63] SARs and currency transaction reports ("CTRs") are a vital source of information that all MSBs—including VASPs, when applicable—should be generating where appropriate, and filing with FinCEN. These reports may contain leads for law enforcement and information necessary to deter, investigate, and prosecute criminal activity.

Importantly, FinCEN's requirements apply equally to domestic and foreign-located MSBs—even if the foreign-located MSB does not have a physical presence in the United States.[64] The MSB need only do business in whole or substantial part in the United States. In addition, parties become money transmitters, and therefore MSBs, whether they exchange from fiat to convertible virtual currency or from one virtual currency to another virtual currency.[65]

Interaction with the Department of Justice. FinCEN's relationship with the Department of Justice and other law enforcement agencies generally falls into two categories: crime prevention (through compliance requirements that prevent money laundering and terrorist activity) and investigatory assistance (through, for example, the provision of leads for criminal investigations generated by regulatory reporting requirements regarding suspicious activity). In addition, FinCEN has the ability to share and to receive financial intelligence information among foreign counterparts, thus creating an important international network. FinCEN also has civil enforcement authority through which it can impose monetary penalties to supplement, or as an alternative to, criminal prosecution in appropriate circumstances, and can take regulatory action to address money laundering and terror financing concerns raised in the virtual currency space.[66]

In just one example of successful collaboration, FinCEN, working in coordination with the United States Attorney's Office for the Northern District of California, assessed a $700,000 civil monetary penalty in 2015 against Ripple Labs Inc. and its wholly-owned subsidiary, XRP II, LLC.[67] Ripple Labs, which is headquartered in San Francisco, facilitated transfers of virtual assets and provided virtual asset exchange transaction services. The company also operated a virtual currency known as XRP that, in 2015, was the second-largest cryptocurrency by market capitalization after Bitcoin. Parallel investigations by the Department of Justice and FinCEN found that Ripple Labs willfully violated several requirements of the BSA by acting as an MSB and selling XRP without registering with FinCEN and by failing to implement and maintain an adequate AML program. Ripple Labs entered into a settlement agreement that resolved possible criminal charges and required the entity to forfeit $450,000. These funds were credited to partially satisfy the $700,000 civil money penalty. In addition, the settlement agreement required Ripple Labs to engage in steps to ensure future compliance with AML/CFT obligations.[68]

[164] For more on the concept of protective jurisdiction in the context of U.S. material support statutes, *see* John De Pue, *Extraterritorial Jurisdiction and the Material Support Statutes*, U.S. Atty's Bulletin, Sept. 2014, available at: https://www.justice.gov/sites/default/files/usao/legacy/2014/09/23/usab6205.pdf (last accessed Oct. 1, 2020).

[165] *See supra* Part I at page 14.

[166] *See supra* Part I at 18, 19.

[167] Verified Complaint for Forfeiture *In Rem*, *United States v. Cazes*, No. 1:17-at-00557, at 21 (E.D. Cal. July 19, 2017), available at: https://www.justice.gov/opa/press-release/file/982821/download (last accessed Oct. 1, 2020).

[168] Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. Dept. of Justice (July 20, 2017), available at: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (last accessed Oct. 1, 2020).

[169] These criminal charges included: narcotics conspiracy (21 U.S.C. §§ 846 and 841(a)(1), (b)(l)(A), (b)(l)(C), 841(h), and 843(b)); distribution of a controlled substance (21 U.S.C. §§ 841(a)(l), (b)(l)(C), & 846); conspiracy to commit identity theft and fraud (18 U.S.C. § 1028(f)); unlawful transfer of a false identification document (18 U.S.C. § 1028(a)(2), (b)(1)(A)(ii), & (f)); conspiracy to commit access device fraud (18 U.S.C. § 1029(b)(2)); trafficking in device making equipment (18 U.S.C. § 1029(a)(4), (b)(l), & (c)(l)(A)(ii)); and money laundering conspiracy (18 U.S.C. § 1956(h)). *See* Indictment, *United States v. Cazes*, Case No, 1:17-CR-00144 (E.D. Cal. June 1, 2017), available at: https://www.justice.gov/opa/press-release/file/982826/download (last accessed Oct. 1, 2020). In addition, prosecutors used various criminal forfeiture statutes (18 U.S.C. §§ 982(a)(l) and 982(a)(2)(B) and 21 U.S.C. § 853(a)). *Id.*

[170] Verified Complaint, *United States v. 280 Virtual Currency Accounts, supra* note 90, at 11.

[171] U.S. Dept. of Justice, Report of the Attorney General's Cyber Digital Task Force 100–01 (July 2018), available at: https://www.justice.gov/cyberreport (last accessed Oct. 1, 2020).

[172] *Id.* at 101.

[173] Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6.1(c) & (f), available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679 (last accessed Oct. 1, 2020).

[174] *Id.*, art. 49.1 & 49.1(d).

[175] Br. of the European Comm'n on Behalf of the E.U. as Amicus Curiae in Support of Neither Party, *United States v. Microsoft*, No. 17-2 (U.S. 2018), available at: https://www.supremecourt.gov/tPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf (last accessed Oct. 1, 2020).

[176] *Id.* at 15.

[177] General Data Protection Regulation, art. 49.1(e), *supra* note 173

[152] *See* 31 C.F.R. §§ 1010.100(ff), 1022.380; *see also* U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, FinCEN Advisory FIN-2012-A001: Foreign-Located Money Services Businesses (Feb. 2012), available at: https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A001.pdf (last accessed Oct. 1, 2020); U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 F.R. 43585 (July 21, 2011), available at http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf (last accessed Oct. 1, 2020).

[153] Many P2P exchange platforms also offer wallet and escrow services, advertising for buyers and sellers, and messaging or chat functions. Generally, platforms that offer hosted wallet services also are MSBs and must comply with the relevant regulations.

[154] *See* 31 U.S.C. §§ 5318 & 5322.

[155] *See supra* Part I at page 14 (discussing KYC requirements).

[156] Press Release, "O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit," U.S. Dept. of Justice, U.S. Att'y's Office, C.D. Cal. (July 22, 2020), available at: https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and (last accessed Oct. 1, 2020).

[157] 31 C.F.R. 1010.100(t)(5)(i).

[158] *See* Press Release, "Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer,' which Laundered Over $300 Million," U.S. Dept. of Justice (Feb. 13, 2020), available at: https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[159] 18 U.S.C. § 1956(a)(1)(B)(i).

[160] Verified Complaint, *United States v. 280 Virtual Currency Accounts*, *supra* note 90, at 11.

[161] Last year, the Law Library of Congress published a comprehensive report on over 40 international jurisdictions' regulatory approaches to cryptoassets, focusing on those jurisdictions' financial market and investor protection laws, as well as on their application of tax and AML/CFT laws. That report confirms the vast diversity of domestic virtual currency regulation, and practice, across the globe. *See* Law Library of Congress, *Regulatory Approaches to Cryptoassets in Selected Jurisdictions* (April 2019), available at: https://www.loc.gov/law/help/cryptoassets/cryptoasset-regulation.pdf (last accessed Oct. 1, 2020).

[162] *See, e.g., United States v. Lord*, 915 F.3d 1009 (5th Cir. 2019); *United States v. Stetkiw*, No. 18-20579, 2019 WL 417404 (E.D. Mich. Feb. 1, 2019); *United States v. Tetley*, No. 17-cr-00738 (C.D. Cal. 2018); *United States v. Mansy*, No. 2:15-cr-198-GZS, 2017 WL 9672554 (D. Maine May 11, 2017); *United States v. Petix*, No. 15-CR-227A, 2016 WL 7017919 (W.D.N.Y. Dec. 1, 2016); *United States v. Noland et al.*, 14-cr-00401-RM (D. Col. 2015); *see also* Press Release, "'Bitcoin Maven' Sentenced to One Year," *supra* note 23.

[163] *United States v. Al Kassar*, 660 F.3d 108, 118 (2d Cir. 2011) (citing *United States v. Peterson*, 812 F.2d 486, 494 (9th Cir. 1987)).

Doe summonses, which require court approval, in certain circumstances "to obtain information about possible violations of internal revenue laws by individuals whose identities are unknown." Press Release, "Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency," U.S. Dept. of Justice (Nov. 30, 2016), available at: https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used (last accessed Oct. 1, 2020).

[139] Rev. Rul. 2019-24, 2019-44 I.R.B. 1004, available at: https://www.irs.gov/pub/irs-drop/rr-19-24.pdf (last accessed Oct. 1, 2020).

[140] Internal Revenue Serv., Frequently Asked Questions on Virtual Currency Transactions, https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions (last accessed Oct. 1, 2020).

[141] *Id.*

[142] N. Am. Sec. Adm'rs Ass'n, *Our Role*, http://www.nasaa.org/about-us/our-role/ (last accessed Oct. 1, 2020).

[143] NASAA, which is comprised of State and territorial securities regulators, has taken an active role in investor education and in coordinating State actions involving VASPs and ICOs. *See, e.g.*, N. Am. Sec. Adm'rs Ass'n, Informed Investor Advisory: Initial Coin Offerings (Apr. 2018), available at https://www.nasaa.org/44836/informed-investor-advisory-initial-coin-offerings/?qoid=investor-education (last accessed Oct. 1, 2020).

[144] News Release, "State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown," N. Am. Sec. Adm'rs Ass'n (May 21, 2018), available at: http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/ (last accessed Oct. 1, 2020).

[145] *See* N.Y. State Office of the Att'y Gen., Virtual Markets Integrity Initiative Report (Sept. 18, 2018), available at: https://virtualmarkets.ag.ny.gov/ (last accessed Oct. 1, 2020).

[146] Press Release, "A.G. Schneiderman Launches Inquiry into Cryptocurrency 'Exchanges,'" N.Y. State Office of the Att'y Gen. (Apr. 17 2018), available at: https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges (last accessed Oct. 1, 2020).

[147] The FATF is also known by its French name, Groupe d'action financière (or "GAFI").

[148] Financial Action Task Force, *What Do We Do*, http://www.fatf-gafi.org/about/whatwedo/ (last accessed Oct. 1, 2020).

[149] FATF International Standards, *supra* note 2, Recommendation 15.

[150] *See id.* at 70–71.

[151] The FATF has undertaken a 12-month review and committed further to a 24-month review of countries' progress with implementing the revised requirements for VASPs. The FATF's 12-month review concluded that there has been progress in implementation of the standards, but that much more remains to be done globally by individual jurisdictions. The report further determined that, while there is no need to revise the standards, there is a need for updated guidance, which the FATF plans to release in 2021. The FATF also undertook a report on so-called "stablecoins" at the request of the G20. This report also found no need to update the FATF standards, but did identify a number of concerns that will be addressed in forthcoming guidance.

[127] *See, e.g., In re Plutus Financial Inc*, CFTC No. 20-23, 2020 WL 4043709 (July 13, 2020) (consent order); *In re BitFinex Inc.*, CFTC No. 16-19, 2016 WL 3137612 (June 2, 2016) (consent order); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015) (consent order).

[128] *In re TeraExchange*, CFTC No. 15-33, 2015 WL 5658082 (Sept. 24, 2015) (consent order).

[129] *CFTC v. 1Pool Ltd*, No. 1:18-cv-2243-TNM, 2019 WL 1605201 (Mar. 4, 2019).

[130] Retail Commodity Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37734 (June 24, 2020) (to be codified at 17 C.F.R. pt. 1).

[131] Press Release, "CFTC Staff Issues Advisory for Virtual Currency Products," Commodity Futures Trading Comm'n (May 21, 2018), available at https://www.cftc.gov/PressRoom/PressReleases/7731-18 (last accessed Oct. 1, 2020).

[132] *See, e.g., CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018).

[133] Press Release, "CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin," Commodity Futures Trading Comm'n (Apr. 18, 2018), available at: https://www.cftc.gov/PressRoom/PressReleases/7714-18 (last accessed Oct. 1, 2020).

[134] Press Release, "Federal Court Orders Defendants to Pay More than $4.25 Million for Fraud and Misappropriation," Commodity Futures Trading Comm'n (Nov. 1, 2019), available at: https://www.cftc.gov/PressRoom/PressReleases/8069-19 (last accessed Oct. 1, 2020).

[135] *See* Indictment, *United States v. Kantor*, No. 18-CR-177 (E.D.N.Y. Apr. 10, 2018), available at: https://www.justice.gov/usao-edny/press-release/file/1053266/download (last accessed Oct. 1, 2020); Press Release, "Defendant Sentenced to 86 Months in Prison for Defrauding Investors in Binary Options and Cryptocurrency Scheme," U.S. Dept. of Justice, U.S. Att'y's Office, E.D.N.Y (July 1, 2019), available at: https://www.justice.gov/usao-edny/pr/defendant-sentenced-86-months-prison-defrauding-investors-binary-options-and (last accessed Oct. 1, 2020).

[136] Notice 2014-21, 2014-16 I.R.B. 938, available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (last accessed Oct. 1, 2020).

[137] Since July 2019, the IRS has sent thousands of warning letters to taxpayers "that potentially failed to report income and pay the resulting tax from virtual currency transactions or did not report their transactions properly." News Release, "IRS has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency's Larger Efforts," Internal Revenue Serv. (July 26, 2019), available at: https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts (last accessed Oct. 1, 2020).

[138] "A John Doe summons is a summons that does not identify the person with respect to whose liability the summons is issued." Internal Revenue Manual, Part 25.5.7, *Special Procedures for John Doe Summonses*, available at: https://www.irs.gov/irm/part25/irm_25-005-007 (last accessed Oct. 1, 2020). The IRS can use John

Defrauding Investors through Two Initial Coin Offerings," U.S. Dept. of Justice, U.S. Att'y's Office, E.D.N.Y (Nov. 15, 2018) (discussing *United States v. Zaslavskiy*, No. 17 CR 647 (RJD) (E.D.N.Y. 2018)), available at: https://www.justice.gov/usao-edny/pr/brooklyn-businessman-pleads-guilty-defrauding-investors-through-two-initial-coin (last accessed Oct. 1, 2020), and Press Release, "Founders Of Cryptocurrency Company Indicted In Manhattan Federal Court With Scheme To Defraud Investors," U.S. Dept. of Justice, U.S. Att'y's Office, S.D.N.Y (May 14, 2018), (discussing *United States v. Sharma, et. al.*, No. 18 Cr. 340 (LGS) (S.D.N.Y. 2019)), available at: https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud (last accessed Oct. 1, 2020).

[118] Press Release, "SEC Halts Alleged Initial Coin Offering Scam," U.S. Sec. and Exch. Comm'n (Jan. 30, 2018), available at: https://www.sec.gov/news/press-release/2018-8 (last accessed Oct. 1, 2020).

[119] Press Release, "Cryptocurrency CEO Indicted After Defrauding Investors of $4 Million," U.S. Dept. of Justice, U.S. Att'y's Office, N.D. Tex. (Nov. 28, 2018), available at: https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million (last accessed Oct. 1, 2020); Indictment, *United States v. Rice*, No. 3:18-CR-587-K (N.D. Tex. Nov. 20, 2018), available at: https://www.justice.gov/usao-ndtx/press-release/file/1115456/download (last accessed Oct. 1, 2020).

[120] Press Release, "Executives Settle ICO Scam Charges," U.S. Sec. and Exch. Comm'n (Dec. 12, 2018), available at: https://www.sec.gov/news/press-release/2018-280 (last accessed Oct. 1, 2020).

[121] 7 U.S.C. § 1 *et seq.*

[122] These terms are defined in the CFTC's Glossary. *See* U.S. Commodity Futures Trading Comm'n, *CFTC Glossary*, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CFTCGlossary/index.htm (last accessed Oct. 1, 2020).

[123] 7 U.S.C. § 1(a)(9).

[124] *See In re Kim*, CFTC No. 19-02, 2018 WL 5993718, at *3 (Oct. 29, 2018) (consent order) ("Virtual currencies such as Bitcoin and Litecoin are encompassed in the definition of 'commodity' under [the CEA]."); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, at *2 (Sept. 17, 2015) (consent order) ("Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities."); *In re TeraExchange LLC*, CFTC No. 15-33, 2015 WL 5658082, at *3 n.3 (Sept. 24, 2015) (consent order) ("Further, bitcoin is a commodity under Section 1a of the Act, 7 U.S.C. § 1a (2012), and is therefore subject as a commodity to applicable provisions of the [CEA] and [CFTC] Regulations.").

[125] *See CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018) ("Virtual currencies can be regulated by CFTC as a commodity. . . . They fall well-within the common definition of 'commodity' as well as the [CEA's] definition of 'commodities' as 'all other goods and articles . . . in which contracts for future delivery are presently or in the future dealt in.'"); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018) (applying a categorical approach to interpreting "commodity" under the CEA and determining that a non-bitcoin virtual currency is a "commodity" under the Act).

[126] U.S. Commodity Futures Trading Comm'n, A CFTC Primer on Virtual Currencies 11 (Oct. 2017), available at: https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf (last accessed Oct. 1, 2020).

[104] The SEC Staff publishes a list of its digital-asset- and ICO-related enforcement actions on its website. *See* U.S. Sec. and Exch. Comm'n, *Cyber Enforcement Actions*, https://www.sec.gov/spotlight/cybersecurity-enforcement-actions (last accessed Oct. 1, 2020); *see also* U.S. Sec. & Exch. Comm'n, *Spotlight on Initial Coin Offerings and Digital Assets*, https://www.investor.gov/additional-resources/spotlight/spotlight-initial-coin-offerings-and-digital-assets (collecting SEC resources on ICOs and other digital-asset-related issues) (last accessed Oct. 1, 2020).

[105] Framework for 'Investment Contract' Analysis of Digital Assets, *supra* note 99.

[106] *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301 (1946).

[107] Framework for 'Investment Contract' Analysis of Digital Assets, *supra* note 99.

[108] The public can engage with SEC Staff through the SEC's Strategic Hub for Innovation and Financial Technology (FinHub). U.S. Sec. and Exch. Comm'n, *FinHub*, www.sec.gov/finhub (last accessed Oct. 1, 2020).

[109] Press Release, "SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering," U.S. Sec. and Exch. Comm'n (Oct. 11, 2019), available at: https://www.sec.gov/news/press-release/2019-212 (last accessed Oct. 1, 2020).

[110] *Id.*

[111] *Id.*

[112] *Id.* In response, Telegram and TON Issuer argued that the sale of Grams to sophisticated investors were lawful private placements of securities covered by an exemption from the registration requirement, and that the anticipated resale of the Grams by those investors to a secondary public market, upon the launch of the TON Blockchain, were unrelated transactions that would not amount to the offer or sale of securities. *See SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, 2020 WL 1430035, at *1 (S.D.N.Y. Mar. 24, 2020).

[113] *Id.*

[114] *Id.*

[115] Final Judgment, *SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, (S.D.N.Y. June 26, 2020), Dkt. No. 242.

[116] For example, in April 2019, the SEC's Division of Corporation Finance provided a "no-action letter" in response to an inquiry from TurnKey Jet, Inc., an interstate air charter services company that proposed "to offer and sell blockchain-based digital assets in the form of 'tokenized' jet cards" without registering under the Securities Act of 1933 or the Securities Exchange Act of 1934. *See* Letter from James P. Curry to SEC Office of Chief Counsel (Apr. 2, 2019), available at: https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1-incoming.pdf (last accessed Oct. 1, 2020). The no-action letter stated that the Division of Corporation Finance would not recommend enforcement action against the company if, based on the facts presented, it offered and sold tokens without registration. *See* TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), available at: https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm (last accessed Oct. 1, 2020).

[117] For examples of prosecutions for securities and other fraud relating to ICOs, see, for example, Press Release, "Brooklyn Businessman Pleads Guilty to

[95] *Id.* at 1.

[96] *Id.* Shortly before this Enforcement Framework was finalized for publication, OCC on September 21, 2020 published an interpretive letter clarifying national banks' and federal savings associations' authority—in certain defined circumstances—to hold "reserves" on behalf of customers who issue certain "stablecoins." ("Stablecoins" are a type of cryptocurrency designed to have a stable value as compared with other types of cryptocurrency, which frequently experience significant volatility.) OCC's Sept. 21 letter represents the latest step in the agency's broader effort to set up systems that will enable banks to adopt cryptocurrency safely. The interpretive letter is available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf (last accessed Oct. 1, 2020).

[97] *See* OCC Consent Order, In re *M.Y. Safra Bank, FSB*, AA-NE-2020-5, at 3 (Jan. 30, 2020), available at: https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf (last accessed Oct. 1, 2020).

[98] U.S. Sec. and Exch. Comm'n, Release No. 81207: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO 10 (July 25, 2017), available at: https://www.sec.gov/litigation/investreport/34-81207.pdf (last accessed Oct. 1, 2020).

[99] U.S. Sec. & Exch. Comm'n Staff, Framework for 'Investment Contract' Analysis of Digital Assets, available at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (last accessed Oct. 1, 2020); Financial Industry Regulatory Authority, *Initial Coin Offerings*, https://www.finra.org/investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/initial-coin-offerings (last accessed Oct. 1, 2020).

[100] The Financial Industry Regulatory Authority (FINRA), which operates under the supervision of the SEC, has issued several investor alerts regarding key cryptocurrency issues, such as ICOs and cryptocurrency-related scams. *See, e.g.*, Financial Industry Regulatory Authority, *Investor Alert, Initial Coin Offerings (ICOs)—What to Know Now and Time-Tested Tips for Investors*, https://www.finra.org/investors/alerts/icos-what-know-now (last accessed Oct. 1, 2020); Financial Industry Regulatory Authority, *Investor Alert, Don't Fall for Cryptocurrency-Related Stock Scams*, https://www.finra.org/investors/alerts/cryptocurrency-related-stock-scams (last accessed Oct. 1, 2020).

[101] SEC Release No. 81207, *supra* note 98.

[102] *Id.* at 17–18; *see also* Jay Clayton [SEC Chairman] and Christopher Giancarlo [CFTC Chairman], *Regulators are Looking at Cryptocurrency*, Wall St. J., Jan. 24, 2018, available at: https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363 ("The SEC does not have direct oversight of transactions in currencies or commodities. Yet some products that are labeled cryptocurrencies have characteristics that make them securities. The offer, sale and trading of such products must be carried out in compliance with securities law.") (last accessed Oct. 1, 2020).

[103] Section 12(k)(1) of the Securities Exchange Act provides the SEC with authority "summarily to suspend trading in any security," other than certain exempted securities, "for a period not exceeding 10 business days" if doing so is, in the SEC's opinion, "in the public interest" and required for "the protection of investors." 15 U.S.C. § 78l(k)(1).

[82] Press Release, "Treasury Sanctions Russia-Linked Election Interference Actors," U.S. Dept. of the Treasury (Sept. 10, 2020), available at: https://home.treasury.gov/news/press-releases/sm1118 (last accessed Oct. 1, 2020).

[83] Press Release, "Russian Project Lakhta Member Charged with Wire Fraud Conspiracy," U.S. Dept. of Justice (Sept. 10, 2020), available at: https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy (last accessed Oct. 1, 2020); see also Indictment, *United States v. Netyksho et al.*, Case No. 18-cr-00215 (D.D.C. 2018), available at: https://www.justice.gov/file/1080281/download (alleging Russian intelligence officers' use of cryptocurrency to launder funds used in furtherance of U.S. election-related hacking activity) (last accessed Oct. 1, 2020).

[84] *See supra* note 32 and accompanying text.

[85] Press Release, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Dept. of the Treasury (Mar. 2, 2020), available at: https://home.treasury.gov/news/press-releases/sm924 (last accessed Oct. 1, 2020).

[86] Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack," U.S. Dept. of Justice (Mar. 2, 2020), available at: https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack (last accessed Oct. 1, 2020); Indictment, *United States v. Yinyin*, No. 1:20-cr-00052-TJK (D.D.C. Feb. 27, 2020), available at: https://www.justice.gov/opa/press-release/file/1253486/download (last accessed Oct. 1, 2020) (charging two Chinese nationals with conspiracy to launder monetary instruments under 18 U.S.C. § 1956(h) and operating an unlicensed money transmitted business under 18 U.S.C. § 1960(a), and seeking forfeiture under 18 U.S.C. § 982(a)(1) and 21 U.S.C. § 853(p)). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[87] Press Release, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts," *supra* note 34.

[88] Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million," *supra* note 86.

[89] Press Release, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts," *supra* note 34.

[90] Verified Complaint, *United States v. 280 Virtual Currency Accounts*, Civ. No. 20-2396, at 11–12 (D.D.C. Aug. 27, 2020), available at: https://www.justice.gov/opa/press-release/file/1310421/download (last accessed Oct. 1, 2020).

[91] Verified Complaint, *United States v. 113 Virtual Currency Accounts*, Civ. No. 20-606, at 4 (D.D.C. Mar. 2, 2020), available at: https://www.justice.gov/opa/press-release/file/1253491/download (last accessed Oct. 1, 2020).

[92] *Id.* at 5.

[93] Office of the Comptroller of the Currency, *What We Do*, https://www.occ.treas.gov/about/index-about.html (last accessed Oct. 1, 2020).

[94] OCC Interpretative Letter #1170, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers* (July 22, 2020), available at: https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (last accessed Oct. 1, 2020).

Oct. 1, 2020); *see also* Press Release, "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK (July 26, 2017), available at: https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf (last accessed Oct. 1, 2020).

[69] *See generally* U.S. DEP'T OF THE TREASURY, *Office of Foreign Assets Control—Sanctions Programs and Information*, https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (last accessed Oct. 1, 2020).

[70] OFAC uses the term "digital currency," which includes cryptocurrency and blockchain-based tokens.

[71] U.S. DEP'T OF THE TREASURY, *Resource Center, OFAC FAQs: Sanctions Compliance*, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx (last accessed Oct. 1, 2020).

[72] *Id.*

[73] *Id.*

[74] OFAC typically uses Executive Orders to designate persons or entities.

[75] Press Release, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," U.S. DEPT. OF THE TREASURY (Nov. 28, 2018), available at: https://home.treasury.gov/news/press-releases/sm556 (last accessed Oct. 1, 2020). For further discussion of the SamSam ransomware scheme, see *supra* page 8.

[76] Press Release, "Treasury Designates Iran-Based Financial Facilitators," *supra* note 75 ("While OFAC routinely provides identifiers for designated persons, today's action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses.").

[77] *Id.*

[78] Press Release, "Two Iranian Men Indicted," *supra* note 17; Indictment, *United States v. Savandi et al.*, No. 18-CR-704 (BRM) (D.N.J. Nov. 26, 2018), available at: https://www.justice.gov/opa/press-release/file/1114741/download (last accessed Oct. 1, 2020).

[79] Press Release, "Treasury Targets Chinese Drug Kingpins Fueling America's Deadly Opioid Crisis," U.S. DEPT. OF THE TREASURY (Aug. 21, 2019), available at: https://home.treasury.gov/news/press-releases/sm756 (last accessed Oct. 1, 2020).

[80] Press Release, "Chinese National Indicted in Southern District of Mississippi Designated by U.S. Treasury Department as Significant Foreign Narcotics Trafficker," U.S. DEPT. OF JUSTICE (Aug 22, 2019), available at: https://www.justice.gov/usao-sdms/pr/chinese-national-indicted-southern-district-mississippi-designated-us-treasury (last accessed Oct. 1, 2020).

[81] Press Release, "Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths," U.S. DEPT. OF JUSTICE (Aug 22, 2018), available at: https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy (last accessed Oct. 1, 2020).

financial-intelligence-units-fius (last accessed Oct. 1, 2020).

[55] U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, FinCEN Guidance FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 7 (May 9, 2019), available at: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (last accessed Oct. 1, 2020).

[56] 76 Fed. Reg. 43585 (2011); *see also* 31 CFR § 1010.100(ff)(5)(A) (emphasis added).

[57] 74 Fed. Reg. 22129, 22137 (2009).

[58] Press Release, "FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities," U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, (Mar. 18, 2013), available at: https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities (last accessed Oct. 1, 2020).

[59] *See* FinCEN Guidance FIN-2013-G001, *supra* note 4.

[60] *Id.*

[61] *See generally* 31 C.F.R. Part 1022 (setting out BSA requirements applicable to MSBs).

[62] *See* FinCEN Guidance FIN-2019-G001, *supra* note 55.

[63] *See id.* at 12.

[64] *Id.*; *see also* 31 CFR § 1010.100(ff).

[65] The 2013 FinCEN guidance notes that a virtual currency exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. *See* FinCEN Guidance FIN-2013-G001, *supra* note 4, at 2. Further, as noted above, an exchanger is a money transmitter if it accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason. *Id.* at 3; *see also* Kenneth A. Blanco, Director, U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), available at: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block (last accessed Oct. 1, 2020).

[66] *See* 31 U.S.C. § 5321 (authorizing the imposition of civil monetary penalties for violations of the BSA); *see also* 31 C.F.R. §§ 1010.820–821.

[67] Press Release, "Ripple Labs Inc. Resolves Criminal Investigation," U.S. Dept. of Justice (May 5, 2015), available at: https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation (last accessed Oct. 1, 2020); Press Release, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger," U.S. Dept. of the Treasury, Fin. Crimes Enf't Network (May 5, 2015), available at: https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual (last accessed Oct. 1, 2020).

[68] In another example of successful coordination, the Department of Justice in 2017 filed criminal charges against MSB BTC-e and its operator (as discussed above), while FinCEN brought a parallel civil enforcement action. *See* Superseding Indictment, *United States v. BTC-e*, No. CR 16-00227 SI (N.D. Cal. Jan. 17, 2017), available at: https://www.justice.gov/usao-ndca/press-release/file/984661/download (last accessed

including an array of illegal narcotics, counterfeit goods and malicious computer hacking software").

[42] Press Release, "J-CODE Announces 61 Arrests in its Second Coordinated Law Enforcement Operation Targeting Opioid Trafficking on the Darknet," FEDERAL BUREAU OF INVESTIGATION (Mar. 26, 2019), available at: https://www.fbi.gov/news/pressrel/press-releases/j-code-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet (last accessed Oct. 1, 2020).

[43] Press Release, "International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million," U.S. DEPT. OF JUSTICE (Sept. 22, 2020), available at: https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170 (last accessed Oct. 1, 2020).

[44] Press Release, "Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," U.S. DEPT. OF JUSTICE (May 8, 2019), available at: https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[45] *Id.*

[46] *See* 18 U.S.C. §§ 2339A & B.

[47] *See* 18 U.S.C. § 792 *et seq.*

[48] 31 C.F.R. § 1010.100(ff).

[49] FATF INTERNATIONAL STANDARDS, *supra* note 2, at 127.

[50] As noted above, "AML/CFT" refers to anti-money laundering and combating the financing of terrorism.

[51] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970). The BSA is the nation's first and most comprehensive federal AML/CFT statute. The Act, which is codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951–1959, and 31 U.S.C. §§ 5311–5314 and 5316–5332, has been amended at various times, including in October 2001 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA PATRIOT Act"). Title III of the USA PATRIOT Act amended the BSA to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Regulations implementing all aspects of the BSA appear at 31 C.F.R. Chapter X.

[52] The authority of the Secretary of the Treasury to administer the BSA and its implementing regulations has been delegated to the Director of FinCEN. Pursuant to this delegation, FinCEN, among other things, develops AML regulations and enforces compliance with the BSA and associated regulations. See Treas. Order 180-01 (July 1, 2014), available at: https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to180-01.aspx (last accessed Oct. 1, 2020).

[53] *See* 31 U.S.C. § 310(c); U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, What is the BSA Data?, https://www.fincen.gov/what-bsa-data (last accessed Oct. 1, 2020).

[54] *See* EGMONT GRP., *Financial Intelligence Units (FIUs)*, https://egmontgroup.org/en/content/

and Homeland Security, along with the Federal Bureau of Investigation, issued an advisory on the cyber threat posed by the North Korean regime. The advisory detailed North Korea's use of state-sponsored cyber actors, including "hackers, cryptologists, and software developers," who, among other things, engage in "cyber-enabled theft targeting financial institutions and digital currency exchanges." U.S. Dept. of Homeland Sec. et al., DPRK Cyber Threat Advisory, *Guidance on the North Korean Cyber Threat* (Apr. 15, 2020), available at: https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf (last accessed Oct. 1, 2020).

[35] Cryptocurrency Crime Losses, *supra* note 33.

[36] Press Release, "Operator Of Bitcoin Investment Platform Pleads Guilty To Securities Fraud And Obstruction Of Justice," U.S. Dept. of Justice, U.S. Att'y's Office, SDNY (July 23, 2018), available at: https://www.justice.gov/usao-sdny/pr/operator-bitcoin-investment-platform-pleads-guilty-securities-fraud-and-obstruction (last accessed Oct. 1, 2020).

[37] Press Release, "Trader Sentenced to 15 Months in Federal Prison for Misappropriating $1.1 Million in Cryptocurrencies," U.S. Dept. of Justice, U.S. Att'y's Office, N.D. Ill. (Nov. 13, 2018), available at: https://www.justice.gov/usao-ndil/pr/trader-sentenced-15-months-federal-prison-misappropriating-11-million-cryptocurrencie-0 (last accessed Oct. 1, 2020).

[38] Norton, *What is Cryptojacking? How It Works and How to Help Prevent It*, https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html (last accessed Oct. 1, 2020).

[39] The aforementioned April 2020 U.S. government advisory regarding North Korea's cyber-hacking program discussed the regime's potential involvement in multiple cryptojacking schemes. *See* DPRK Cyber Threat Advisory, *supra* note 34 at 2. Specifically, the advisory noted "several incidents in which computers infected with cryptojacking malware sent the mined assets—much of it anonymity-enhanced digital currency (sometimes also referred to as 'privacy coins')—to servers located in [North Korea]." *Id.* (citing a report by a UN Security Council panel of experts); *see also, e.g.*, Timothy W. Martin, *New North Korea Hack: Hijacking Computers to Power Cryptocurrency Mining*, Wall St. J., Jan. 8, 2018, available at: https://www.wsj.com/articles/in-north-korea-hackers-mine-cryptocurrency-abroad-1515420004?mod=article_inline (last accessed Oct. 1, 2020).

[40] Press Release, "Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," U.S. Dept. of Justice (May 8, 2019), available at: https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[41] *See* Press Release, "3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges," U.S. Dept. of Justice, U.S. Att'y's Office, C.D. Cal. (May 3, 2019), available at: https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us (last accessed Oct. 1, 2020) (describing criminal complaint against the alleged administrators of Wall Street Market (WSM), "one of the world's largest dark web marketplaces that allowed vendors to sell a wide variety of contraband,

[28] Press Release, "Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," U.S. Dept. of Justice, U.S. Att'y's Office, N.D. Cal. (July 26, 2017), available at: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[29] For other examples of cases in which virtual currency exchanges have been charged with operating an unlicensed money transmitting business, *see United States v. Murgio*, 15-cr-769(AJN), 2017 WL 365496 (S.D.N.Y. Jan. 20, 2017) and *United States v. Faiella*, 39 F. Supp. 3d 544 (S.D.N.Y. 2014). *See also United States v. Budovsky*, No. 13-cr-368 (DLC), 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (noting that 18 U.S.C. § 1960, which covers operation of an unlicensed money transmitting business, encompasses businesses that transmit virtual currency).

[30] *See* I.R.S. Notice 2014-21, available at: https://www.irs.gov/pub/irs-drop/n-14-21.pdf (last accessed Oct. 1, 2020).

[31] Press Release, "Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela," U.S. Dept. of the Treasury (Mar. 11, 2019), available at: https://home.treasury.gov/news/press-releases/sm622 (last accessed Oct. 1, 2020).

[32] *See generally, e.g.*, Yaya J. Fanusie & Trevor Logan, *Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance*, Found. for Def. of Democracies (July 2019), available at: https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf (last accessed Oct. 1, 2020). While publicly available details remain scarce, reports indicate that North Korea also has been active in exploiting cryptocurrency technology in part because of "a desire to avoid crippling international sanctions." Megan McBride & Zack Gold, *Cryptocurrency: Implications for Special Operations Forces* at 30, CNA (Aug. 2019), available at: https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf (last accessed Oct. 1, 2020); see also *Crypto Rogues*, *supra*, at 8 n.4 ("North Korea is also trying to obtain cryptocurrencies to offset sanctions mostly through cyber theft.").

[33] Gertrude Chavez-Dreyfuss, *Cryptocurrency Crime Losses More than Double to $4.5 Billion in 2019, Report Finds*, Reuters, Feb. 11, 2020, available at: https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-losses-more-than-double-to-45-billion-in-2019-report-finds-idUSKBN2051VT (last accessed Oct. 1, 2020).

[34] As discussed further in the text, the Department of Justice recently brought criminal charges against two individuals accused of laundering over $100 million worth of cryptocurrency allegedly stolen by North Korean hacks of cryptocurrency exchanges. The Department also filed a civil forfeiture complaint that "publicly exposes the ongoing connections between North Korea's cyber-hacking program and a Chinese cryptocurrency money laundering network." Press Release, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors," U.S. Dept. of Justice (August 27, 2020), available at: https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges (last accessed Oct. 1, 2020). In April 2020, the U.S. Departments of State, Treasury,

Municipalities, and Public Institutions, Causing Over $30 Million in Losses," U.S. Dept. of Justice (Nov. 28, 2018), available at: https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[18] Press Release, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," U.S. Dept. of Justice (Oct. 16, 2019), available at: https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[19] Indictment, *United States v. Mohammad*, No. 20-cr-0065, at 6 (DLF) (D.D.C. March 2020), available at: https://www.justice.gov/usao-dc/press-release/file/1257641/download (last accessed Oct. 1, 2020); *see also* Press Release, "Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 'Real Rape' and Child Pornography Videos, Funded by Cryptocurrency," U.S. Dept. of Justice (Mar. 12, 2020), available at: https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[20] Verified Complaint for Forfeiture In Rem, *United States v. Three Hundred Three Virtual Currency Accounts et. al.*, No. 20-cv-712 (D.D.C. Mar. 12, 2020), available at: https://www.justice.gov/usao-dc/press-release/file/1257581/download (last accessed Oct. 1, 2020).

[21] Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," *supra* note 16.

[22] Verified Complaint for Forfeiture *In Rem*, *United States v. One Hundred Fifty Five Virtual Currency Assets*, No. 20-cv-2228 (D.D.C. Aug. 13, 2020), available at: https://www.justice.gov/opa/press-release/file/1304296/download (last accessed Oct. 1, 2020).

[23] Press Release, "'Bitcoin Maven' Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case," U.S. Dept. of Justice, U.S. Att'y's Office, C.D. Cal. (July 9, 2018), available at: https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case (last accessed Oct. 1, 2020).

[24] The federal crime of money laundering is defined in 18 U.S.C. § 1956.

[25] AML/CFT standards are discussed further in Part II.

[26] *See* FinCEN Guidance FIN-2013-G001, *supra* note 4, at 2; *see also* Virtual Currencies: Key Definitions and Potential AML/CFT Risks, *supra* note 4, at 7.

[27] Press Release, "'Bitcoin Maven' Sentenced to One Year," *supra* note 23.

United States v. Colldock, No. CR-16-1254-JAS, 2017 WL 9615895 (D. Ariz. Sept. 11, 2017) (methamphetamine and cocaine); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016) (child pornography); *United States v. Parks*, No. S1-4:15 CR 553, 2016 WL 6775465 (E.D. Mo. Sept. 19, 2016) (human trafficking and prostitution); *United States v. 50.44 Bitcoins*, No. ELH-15-3692, 2016 WL 3049166 (D. Md. May 31, 2016) (narcotics and illicit Bitcoin-to-fiat-currency exchanges); and *United States v. Donagal*, No. 14–cr–00285–JST–1, 2014 WL 6601843 (N.D. Cal. Nov. 18, 2014) (illegally manufactured Xanax, GHB, steroids, and other drugs).

[10] *See infra* pages 7-20 (describing AlphaBay, Operation DisrupTor, terrorist financing cases, and other examples).

[11] For example, in 2017, the U.S. government formally asserted that North Korea conducted a massive ransomware attack, referred to as the WannaCry attack, which infected computers around the world. The perpetrators of the WannaCry attack demanded ransom payments from their victims in Bitcoin. *See, e.g.*, Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, Wall St. J., Dec. 18, 2017, available at: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 (last accessed Oct. 1, 2020).

[12] Press Release, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," Federal Bureau of Investigation (Apr. 13, 2020), available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic#:~:text=FBI%20Expects%20a%20Rise%20in%20Scams%20Involving%20Cryptocurrency%20Related%20to,through%20the%20complex%20cryptocurrency%20ecosystem (last accessed Oct. 1, 2020).

[13] *See infra* page 16.

[14] In what was reported in January 2015 as the "first instance of an ISIS cell fundraising using Bitcoin on the dark web," the FBI shut down the online cryptocurrency account of a known ISIS fundraiser, Abu Mustafa. Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, & Julia Solomon-Strauss, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Ctr. for a New Am. Sec., May 2017, at 12, available at: https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819 (last accessed Oct. 1, 2020); *see also* European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, *Virtual Currencies and Terrorist Financing: Assessing Risks and Evaluating Responses*, May 2018, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (providing detailed threat assessment, describing European Union's response, and setting out policy recommendations) (last accessed Oct. 1, 2020).

[15] Press Release, "Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL," U.S. Dept. of Justice (Aug. 28, 2015), available at: https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil (last accessed Oct. 1, 2020).

[16] Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," U.S. Dept. of Justice (Aug. 13, 2020), available at: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (last accessed Oct. 1, 2020).

[17] *See* Press Release, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals,

[4] U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, FinCEN Guidance FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), available at: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (last accessed Oct. 1, 2020). A non-convertible virtual currency may effectively become a convertible virtual currency where a robust unofficial secondary market for the currency develops and provides the opportunity to exchange the "non-convertible" currency for fiat or other virtual currency. *See* Financial Action Task Force (FATF), Virtual Currencies: Key Definitions and Potential AML/CFT Risks 4–5 (June 2014), available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (last accessed Oct. 1, 2020).

[5] Throughout this publication, specific examples of cryptocurrency, like Bitcoin, are capitalized when referring to the protocol, and lowercase when referring to units of the cryptocurrency.

[6] To the extent this Framework discusses or references criminal cases that are pending at the time of publication, it should be noted that criminal charges are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[7] For example, Christopher Bantli, a Canadian citizen, used cryptocurrency while acting as a vendor of controlled substances on the darknet website AlphaBay. In February 2019, Bantali pleaded guilty in U.S. federal court to accepting virtual currency as payment for controlled substances, including powerful fentanyl analogues and synthetic opiates. *See* Press Release, "Dark Web Trafficker Convicted of Drug Importation Conspiracy," U.S. Dept. of Justice (Feb. 13, 2019), available at: https://www.justice.gov/opa/pr/dark-web-trafficker-convicted-drug-importation-conspiracy (last accessed Oct. 1, 2020).

[8] In October 2018, Ammar Atef Alahdali pleaded guilty to receipt of child pornography after admitting to paying cryptocurrency to become a member of a darknet website dedicated to the advertisement and distribution of such illicit material. In 2017, Alahdali used the website to download more than twenty images depicting the sexual abuse of children, including at least one video depicting sadistic sexual conduct. *See* Press Release, "Foreign National Pleads Guilty to Downloading Child Pornography from the Dark Web in Exchange for Cryptocurrency," U.S. Dept. of Justice (Oct. 2, 2018), available at: https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-downloading-child-pornography-dark-web-exchange-cryptocurrency (last accessed Oct. 1, 2020).

[9] For examples of cases where cryptocurrencies were used in the illicit sales on the dark web, *see, e.g., United States v. Hagan*, 766 Fed. Appx. 356 (6th Cir. 2019) (MDMA, LSD, DMT, mushrooms, and marijuana); *United States v. Reuer*, CR. 19-50022-JLV, 2019 WL 1012187 (D.S.D. Mar. 4, 2019) (methamphetamine, fentanyl, and heroin); *State v. Sawyer*, 187 A.3d 377 (Vt. 2018) (firearms); *State v. A.P.*, 117 N.E.3d 840 (Ohio 2018) (LSD); *United States v. 2013 Lamborghini Aventador*, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018) (luxury vehicles); *United States v. Michell*, No. CR-17-01690-001-PHX-GMS, 2018 WL 2688803 (D. Ariz. June 5, 2018) (potassium cyanide and dimethyl mercury); *United States v. Vallerius*, No. 17-CR-20648, 2018 WL 2325729 (S.D. Fla. May 1, 2018) (narcotics); *United States v. Focia*, 869 F.3d 1269 (11th Cir. 2017) (firearms); *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) (drugs, false identification documents, and computer hacking software);

NOTES

Introduction

[i] The original formulation of this phrase (describing the laws as "those wise restraints that make men free") was coined by Professor John MacArthur Maguire of Harvard. *See* https://asklib.law.harvard.edu/faq/115309 (last accessed Oct. 1, 2020).

[ii] Jeff Sessions, Attorney General, "Memorandum for Heads of Department Components [Establishing Cyber-Digital Task Force]," Feb. 16, 2018, available at: https://www.justice.gov/opa/press-release/file/1035457/download (last accessed Oct. 1, 2020).

[iii] U.S. Dep't of Justice, Report of the Attorney General's Cyber-Digital Task Force 126 (2018), available at: https://www.justice.gov/cyberreport (last accessed Oct. 1, 2020).

[iv] U.S. Dep't of Commerce, Nat'l Inst. of Standards and Tech., "Blockchain," available at: https://www.nist.gov/topics/blockchain (last accessed Oct. 1, 2020).

[v] U.S. Dep't of Def, "DoD Digital Modernization Strategy," at 44 (Appendix I), July 12, 2019, available at: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF (last accessed Oct. 1, 2020).

[vi] *See* U.S. Food and Drug Admin., "New Era of Smarter Food Safety: FDA's Blueprint for the Future," July 2020, available at: https://www.fda.gov/media/139868/download (last accessed Oct. 1, 2020).

[vii] Lael Brainard, Fed. Reserve Governor, "An Update on Digital Currencies," Aug. 13, 2020, available at: https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm (last accessed Oct. 1, 2020).

[viii] Binance, "The Evolution of the Internet – Web 3.0 Explained," Feb. 2020, available at: https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained (last accessed Oct. 1, 2020).

Cryptocurrency: An Enforcement Framework

[1] Ctrs. for Disease Control & Prevention, *Drug Overdose Deaths*, https://www.cdc.gov/drugoverdose/data/statedeaths.html (last accessed Oct. 1, 2020).

[2] Financial Action Task Force (FATF), The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 126 (June 2019) [hereinafter FATF International Standards], available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (last accessed Oct. 1, 2020).

[3] Some countries, including the United States (see text accompanying *supra* note vii), are exploring the use of blockchain technology to support a national currency. Such currencies are sometimes referred to as "Central Bank Digital Currencies" or "CBDCs." *See, e.g.*, PricewaterhouseCoopers, The Rise of Central Bank Digital Currencies (CBDCs) 2 (Nov. 2019), available at: https://www.pwc.com/gx/en/financial-services/pdf/the-rise-of-central-bank-digital-currencies.pdf (last accessed Oct. 1, 2020).

thereby harming the interests of the United States and its allies.

Despite the many challenges, the Department of Justice has aggressively investigated and prosecuted a range of malign actors who have used cryptocurrencies to facilitate or to conceal their illicit activities. Similarly, the Department has brought actions against individuals and companies that have failed to meet their legal obligations to counter illicit activity. In particular cases, we have even proceeded against the illicit cryptocurrency itself, seizing those virtual assets and removing them from the stream of international commerce, irrespective of our ability to identify or to apprehend the actors who used them. This essential work will continue, as the Department seeks to ensure that uses of cryptocurrency adhere to the law and are compatible with the protection of public safety and national security.

The Department of Justice, however, cannot achieve success on its own. We recognize the importance of working with interagency and international partners to enhance an already vigorous enforcement plan, regulatory scheme, and policy framework to thwart the opportunities created by cryptocurrency for criminals, terrorists, and other bad actors. The Department is committed to strengthening its key partnerships by promoting law enforcement awareness and expertise; by fostering cooperation with State authorities; by enhancing international cooperation; by promoting comprehensive, consistent international regulation; and by conducting private sector education and outreach.

To promote public safety and protect national security, all stakeholders—from private industry to regulators, elected officials, and individual cryptocurrency users—will need to take steps to ensure cryptocurrency is not used as a platform for illegality. Indeed, for cryptocurrency to realize its truly transformative potential, it is imperative that these risks be addressed.

The Department also works with its partners in the federal government to encourage their international counterparts to continue development of comprehensive and consistent international regulation of virtual assets. As discussed above, the Financial Action Task Force has adopted amendments to its Recommendation 15 that bring VASPs and virtual asset activity within the FATF's standards for AML/CFT. As implementation of these amendments expands across global jurisdictions, the Department will continue to provide policy support and subject matter expertise to the Department of the Treasury-led U.S. delegation, and to work internationally to level the legal and regulatory playing field related to virtual assets. In addition, other international organizations, including the United Nations Office on Drugs and Crime, are in the process of adopting regulatory frameworks that mirror the FATF's developing approach to virtual asset activity. We will monitor and actively contribute to those efforts, as appropriate.

Finally, the Department will continue to encourage its partners to support the adoption of consistent regulations across jurisdictions to prevent illicit actors from practicing jurisdictional arbitrage, and to ensure the collection of important evidence and seizure of illicit assets regardless of where an entity or illicit actor may be operating.

Conducting private sector education and outreach. As with any specialized, technology-driven industry, effective regulation and policing of cryptocurrency activity requires close cooperation between the public and private sectors whenever possible. This approach includes direct engagement with the companies that operate in the virtual asset space; with the banks and financial institutions that may be affected by virtual asset regulation; and, importantly, with the actual community of cryptocurrency users. In conducting such outreach, the Department and its partners will continue their efforts to advance mutual goals such as safeguarding the virtual asset marketplace from theft, fraud, and hacking.

Conclusion

As the use of cryptocurrency evolves and expands, so too will opportunities to commit crime and to do harm by exploiting cryptocurrency technology. Every day, criminals expand and perfect techniques designed to evade detection and apprehension. Ultimately, illicit uses of cryptocurrency threaten not just public safety, but national security, as well. For example, cryptocurrency can provide terrorist organizations a tool to circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions. Current terrorist use of cryptocurrency may represent the first raindrops of an oncoming storm of expanded use that could challenge the ability of the United States and its allies to disrupt financial resources that would enable terrorist organizations to more successfully execute their deadly missions or to expand their influence.

Likewise, cryptocurrency presents a troubling new opportunity for individuals and rogue states to avoid international sanctions and to undermine traditional financial markets,

THE GDPR

In May 2018, the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR") came into effect. GDPR is a sweeping data protection and privacy law that applies to all data controllers, data processors, and data subjects within the EU's jurisdiction. Some virtual currency exchanges have attempted to withhold data requested by law enforcement agencies in the United States through criminal grand jury subpoenas by citing GDPR's broad privacy rules.

However, GDPR does not in fact bar companies subject to U.S. jurisdiction from complying with lawful requests in criminal investigations. To the contrary, GDPR explicitly permits the disclosure of data in a number of scenarios. For example, a virtual exchange that is subject to GDPR may process the requested data under GDPR Article 6(1) when "necessary for compliance with a legal obligation to which the controller is subject" or "necessary for the purposes of the legitimate interests pursued by the controller or by a third party . . . ."[173] Similarly, under Article 49.1, international transfer of data is permitted in various circumstances, including where "the transfer is necessary for important reasons of public interest" or "necessary for the purposes of compelling legitimate interests pursued by the controller."[174]

The ability of law enforcement to investigate criminal activity is plainly an important reason of public interest, placing production of records pursuant to U.S. grand jury subpoenas squarely within the "public interest" exception in Article 49.1. Moreover, the transfer of data from exchanges may constitute a "compelling legitimate interest" in that the transfer may be necessary to prevent or defend against being held in contempt of court for failure to respond to lawful process. Indeed, the European Commission itself recognized this framework in a 2017 amicus brief it filed in the U.S. Supreme Court in *United States v. Microsoft*,[175] which discussed the GDPR's rules governing the transfer of personal data to a non-EU state. In its brief, the European Commission recognized that the public interest is served by transferring data to non-EU countries to further international criminal investigations, stating: "[I]n general, [European] Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest."[176]

GDPR Articles 6 and 49.1 provide additional legal bases for processing and transfer that may be applicable in particular circumstances. For example, Article 49.1(e) establishes a derogation if "the transfer is necessary for the establishment, exercise or [defense] of legal claims."[177] This derogation may be applicable where the transfer of data from exchanges is sought pursuant to a subpoena or other compulsory order.

While the Department disagrees with the basis for such objections to lawful requests for information, some exchanges continue to cite to the GDPR while refusing to comply with standard grand jury subpoenas. The Department will continue to engage with these virtual currency exchanges to ensure compliance with lawful requests and will pursue motions to compel as needed.

THE DIGITAL CURRENCY INITIATIVE

As announced in the July 2018 Report of the Attorney General's Cyber Digital Task Force, the Money Laundering and Asset Recovery Section ("MLARS") within the Department of Justice's Criminal Division has established a Digital Currency Initiative to focus on "providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfeitures."[171] The Digital Currency Initiative continues to "expand and implement cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department components to pursue such cases, while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture."[172]

consider legislative proposals to close any existing gaps in enforcement authority.

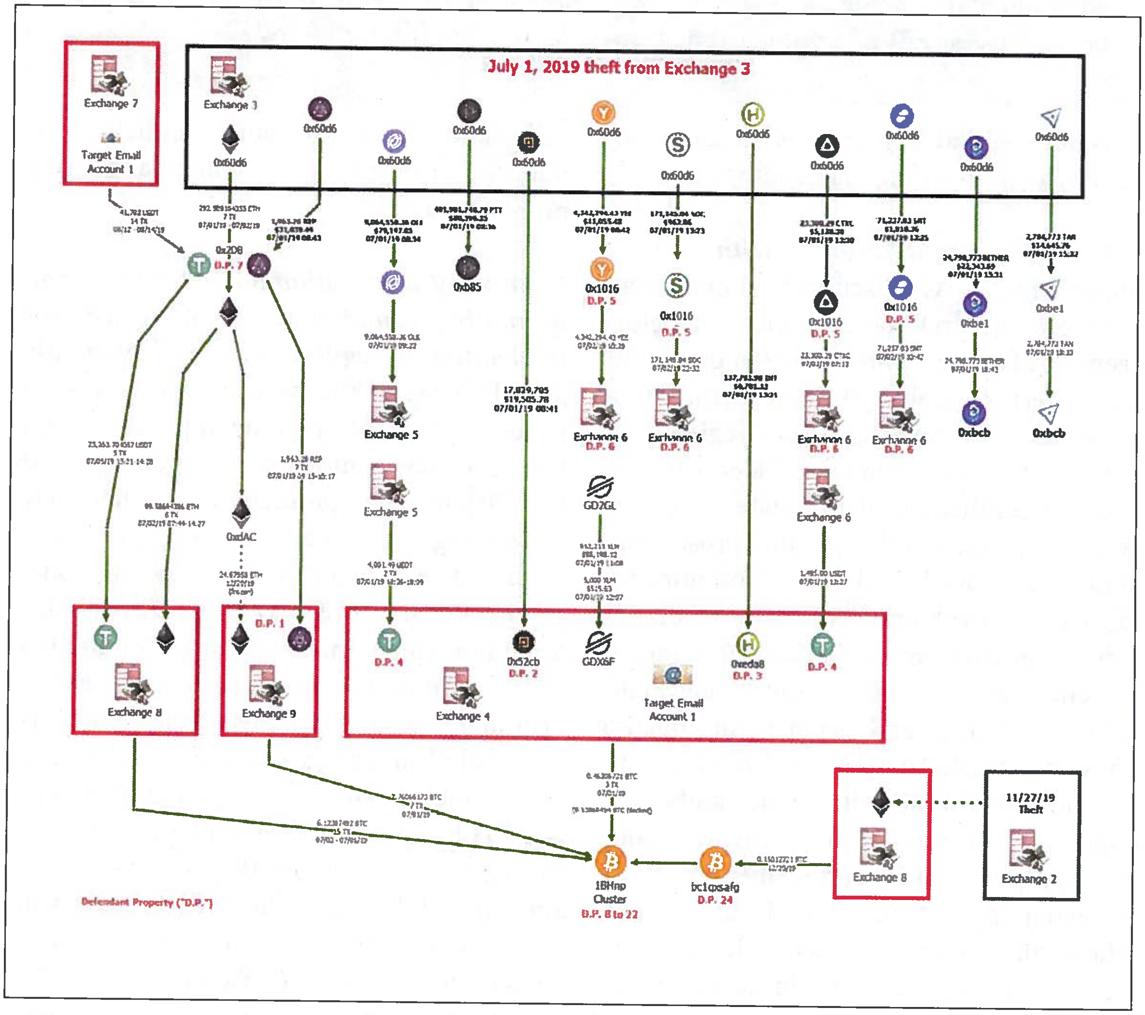
Fostering cooperation with State authorities. As discussed above, State attorneys general offices and regulatory agencies play an important role in protecting the investing public by enforcing State securities laws and licensing, registration, and auditing requirements. Coordination and de-confliction with State attorneys general offices, regulators, and prosecuting entities is crucial, and yet communication on matters involving virtual assets between federal prosecutors and State authorities currently varies by jurisdiction. United States Attorneys' Offices and Department litigating divisions should continue to develop lines of communication with State authorities handling securities and fraud investigations, prosecutions, and enforcement actions involving cryptocurrency and virtual-asset-related investment products. In addition, Department agencies should communicate and coordinate with State financial and banking authorities that regulate money transmitters operating in their respective jurisdictions to prevent conflicts and duplication of efforts in money laundering prosecutions.

Enhancing international cooperation and promoting comprehensive and consistent international regulation. The inherently global nature of the virtual asset ecosystem poses significant investigative challenges for U.S. law enforcement agencies and for Department prosecutors. Effectively countering criminal activity involving virtual assets requires close international partnerships. Foreign partners assist U.S. law enforcement in, for example, conducting investigations, making arrests, and seizing criminal assets. Similarly, foreign partners may rely on the assistance of U.S. law enforcement to take action against individuals who commit crimes abroad and conceal evidence and assets—or themselves—within the United States. The Department will continue to encourage these partnerships in support of multi-jurisdictional parallel investigations and prosecutions, particularly those involving foreign-located actors, VASPs, and transnational criminal organizations.

formalized training of investigators and prosecutors on the cryptocurrency threat and how best to address it; working with federal, State, local, and international partners to promote and coordinate the sharing of information and resources; serving as the main point of contact in cross-jurisdictional investigations; and conducting outreach to the private sector in support of public-private partnerships.

The Department also will work with law enforcement agencies to develop further strategic guidance on the use of available legal tools to investigate and prosecute cryptocurrency-related offenses, and

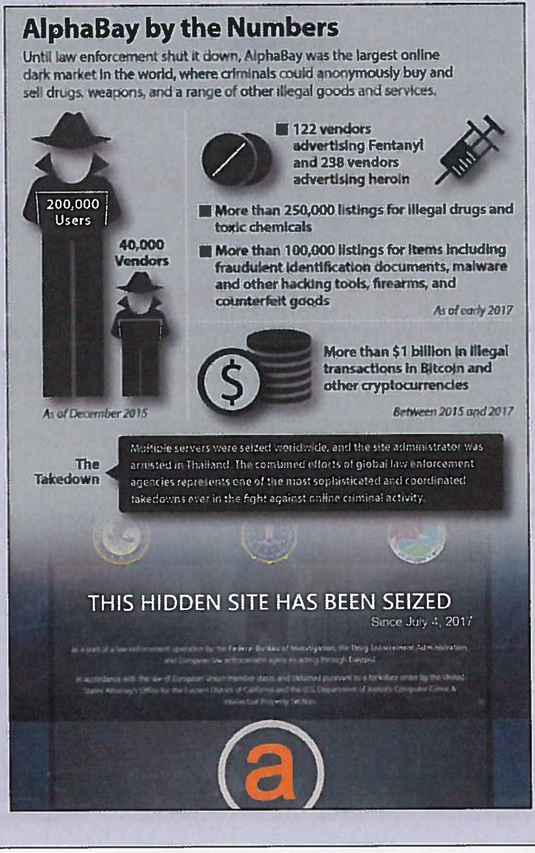
Figure 18: Example of an Illicit Transaction Path Developed Through Blockchain Analysis[170]



This chart depicts a complex series of transactions following a theft from a virtual currency exchange ("Exchange 3"), including numerous conversions of cryptocurrency and deposits and withdrawals involving several intermediary addresses and exchanges. Successful investigations of such schemes require enhanced training and technical capabilities.

CASE STUDY: AlphaBay

The AlphaBay case, which also was mentioned previously,[166] further demonstrates the global reach of the Department of Justice, U.S. law enforcement, and our domestic and international partners in identifying and neutralizing unlawful activities involving cryptocurrency. At the time of its takedown by law enforcement in July 2017, AlphaBay was the dark web's largest criminal marketplace, serving over 200,000 users as a conduit for everything from illegal drugs and firearms to malware and toxic chemicals. Aided by the use of cryptocurrencies like Bitcoin, Monero, and Ether, AlphaBay's operators were able to hide the location and identities of the site's administrators and users and to facilitate the laundering of hundreds of millions of dollars. Over the course of the government's investigation, law enforcement identified AlphaBay proceeds and discovered hundreds of thousands of cryptocurrency addresses associated with the site.[167] The international operation to dismantle AlphaBay was led by the United States and involved cooperation from law enforcement partners in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.[168] The legal proceedings in the United States demonstrated the breadth of authorities the Department can and will bring to bear in appropriate cases.[169]



AlphaBay by the Numbers

Until law enforcement shut it down, AlphaBay was the largest online dark market in the world, where criminals could anonymously buy and sell drugs, weapons, and a range of other illegal goods and services.

- 122 vendors advertising Fentanyl and 238 vendors advertising heroin
- More than 250,000 listings for illegal drugs and toxic chemicals
- More than 100,000 listings for items including fraudulent identification documents, malware and other hacking tools, firearms, and counterfeit goods

As of early 2017

More than $1 billion in illegal transactions in Bitcoin and other cryptocurrencies

Between 2015 and 2017

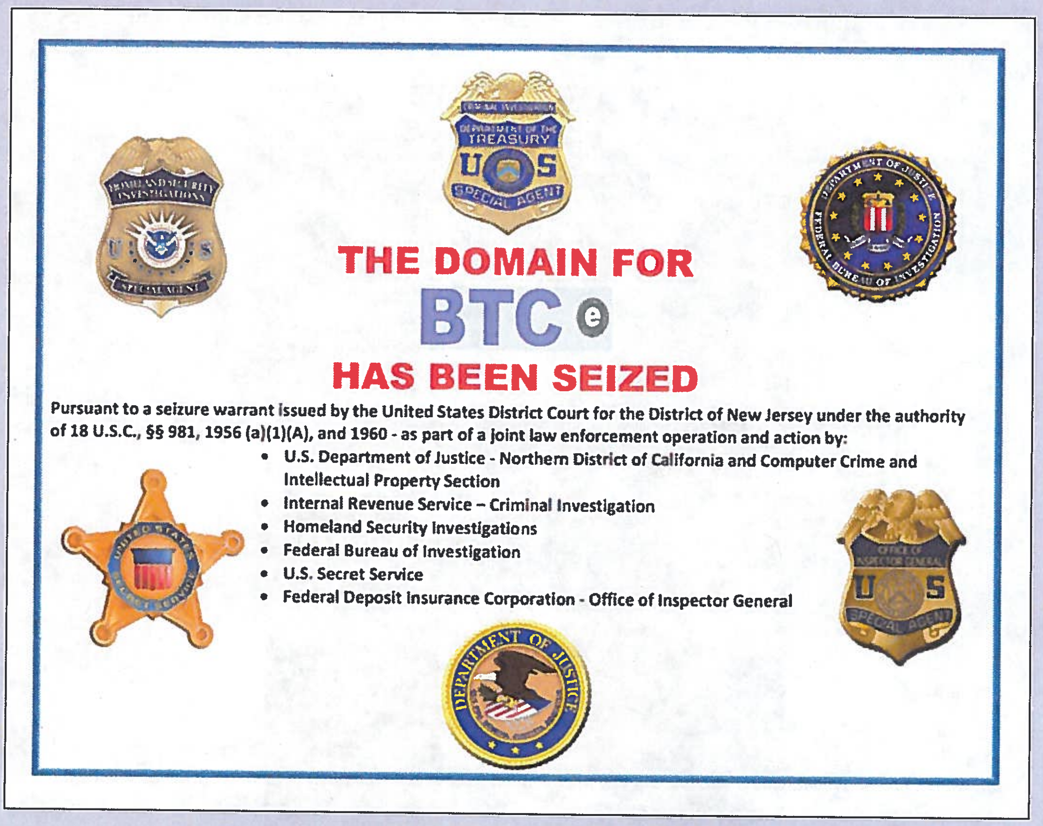
The Takedown: Multiple servers were seized worldwide, and the site administrator was arrested in Thailand. The combined efforts of global law enforcement agencies represents one of the most sophisticated and coordinated takedowns ever in the fight against online criminal activity.

THIS HIDDEN SITE HAS BEEN SEIZED

Since July 4, 2017

CASE STUDY: BTC-e

The BTC-e case, which was introduced earlier,[165] is one example of the Department of Justice's resolve to prosecute foreign-located entities and individuals in the cryptocurrency context. BTC-e operated globally as an unlicensed virtual currency exchange to launder and liquidate criminal proceeds from virtual currency to fiat currency. In doing so, it relied on the use of shell companies and affiliated entities that were similarly unregistered with FinCEN. According to its now-defunct website, BTC-e purported to be based in Eastern Europe. BTC-e's managing shell company, Canton Business Corporation, was registered in the Seychelles, and its web domains were registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand. After a multi-year, multi-agency investigation, the Department successfully charged BTC-e and one of its principal operators with operating an unlicensed money services business, money laundering, and other related crimes.


HOMELAND SECURITY INVESTIGATIONS
U S
SPECIAL AGENT
CRIMINAL INVESTIGATION
DEPARTMENT OF THE TREASURY
U S
SPECIAL AGENT
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
OFFICE OF INSPECTOR GENERAL
U S
SPECIAL AGENT
DEPARTMENT OF JUSTICE

THE DOMAIN FOR

BTC e

HAS BEEN SEIZED

Pursuant to a seizure warrant issued by the United States District Court for the District of New Jersey under the authority of 18 U.S.C., §§ 981, 1956 (a)(1)(A), and 1960 - as part of a joint law enforcement operation and action by:

- U.S. Department of Justice - Northern District of California and Computer Crime and Intellectual Property Section
- Internal Revenue Service – Criminal Investigation
- Homeland Security Investigations
- Federal Bureau of Investigation
- U.S. Secret Service
- Federal Deposit Insurance Corporation - Office of Inspector General

Figure 17: BTC-e Website after Seizure by the U.S. Government

to engage actively with its regulatory partners to address the misuse and abuse of cryptocurrency by malicious actors. The case examples noted throughout this Framework highlight the many successes from the Department's work with regulatory partners such as FinCEN, OFAC, the SEC, the CFTC, and the IRS. By appropriately coordinating parallel enforcement actions, the Department can maximize its impact in investigating, dismantling, and deterring criminal activity; more effectively recover funds for victims; and better safeguard the financial system and the American public.

The Department also has robust authority to prosecute VASPs and other entities and individuals that violate U.S. law even when they are not located inside the United States. Where virtual asset transactions touch financial, data storage, or other computer systems within the United States, the Department generally has jurisdiction to prosecute the actors who direct or conduct those transactions. The Department also has jurisdiction to prosecute foreign-located actors who use virtual assets to import illegal products or contraband into the United States, or use U.S.-located VASPs or financial institutions for money laundering purposes. In addition, the Department may prosecute for violations of U.S. law those foreign-located actors who provide illicit services to defraud or steal from U.S. residents. Moreover, as FinCEN has observed, the BSA applies to entities and individuals that engage in money transmission as a business and that operate wholly or substantially in part in the United States, regardless of where they are incorporated or headquartered.

Finally, it bears emphasizing that if conduct involving virtual currency were to violate the U.S. statutes regarding material support of terrorism, the U.S. government could appropriately assert jurisdiction over such offenses anywhere in the world, consistent with due process, under the principle of protective jurisdiction. That principle holds that "[f]or non-citizens acting entirely abroad, a jurisdictional nexus exists when the aim of that activity is to cause harm inside the United States or to U.S. citizens or interests."[163] Where a malign actor's conduct involving cryptocurrency amounts to providing material support to a designated foreign terrorist organization, that actor engages in conduct that threatens the security of the United States, and therefore subjects himself (or itself) to the jurisdiction of our Nation's courts—and to the Department's enforcement of the Nation's laws.[164]

Promoting law enforcement awareness and expertise. Given the complexity of cryptocurrency technology and of the platforms on which it is used, law enforcement professionals across agencies must continually develop and maintain the base of knowledge and skills necessary to identify threats involving cryptocurrency; conduct robust and efficient investigations of those threats; and employ the many appropriate legal tools available to bring individuals and entities that abuse cryptocurrency to justice. The Department is taking the lead in this area by dedicating resources to existing initiatives and groups that encourage law enforcement awareness and expertise in the cryptocurrency space. These efforts include continuing to promote Department-wide, "conceal or disguise the nature, the location, the source, the ownership, or the control" of a financial transaction.[159]

Criminals also may engage in a practice known as "chain hopping," in which they move from one cryptocurrency to another, often in rapid succession. As the Department has observed, chain hopping is "frequently used by individuals who are laundering proceeds of virtual currency thefts."[160] Chain hopping is often viewed as a potential way to obfuscate the trail of virtual currency by shifting the trail of transactions from the blockchain of one virtual currency to the blockchain of another virtual currency.

Jurisdictional arbitrage and compliance deficiencies. Because of the global and cross-border nature of transactions involving virtual assets, the lack of consistent AML/CFT regulation and supervision over VASPs across jurisdictions—and the complete absence of such regulation and supervision in certain parts of the world—is detrimental to the safety and stability of the international financial system.[161] This inconsistency also impedes law enforcement's ability to investigate, prosecute, and prevent criminal activity involving or facilitated by virtual assets. For example, illicit financial flows denominated in virtual assets may move to companies and exchanges in jurisdictions where authorities lack regulatory frameworks requiring the generation and retention of records necessary to support investigations.

In the United States, AML/CFT standards have been in place for MSBs engaged in virtual asset activities since 2011, and yet many VASPs still are operating in ways that do not comply with the BSA and other regulatory requirements. For example, some VASPs apply different standards to U.S. customers versus customers in other countries, while other VASPs actively apply different standards to virtual-asset-to-fiat transactions than to virtual-asset-to-virtual-asset transactions. Such behaviors are flatly inconsistent with VASPs' BSA obligations and can create significant financial intelligence gaps.

B. Department of Justice Response Strategies

Investigations and prosecutions generally. Consistent with its mission to protect public safety and national security, the Department of Justice will continue its aggressive investigation and prosecution of a wide range of malicious actors, including those who use cryptocurrencies to commit, facilitate, or conceal their crimes. For instance, the Department has prosecuted a number of individuals operating as P2P exchangers for money laundering and for violating the BSA.[162] Many of these exchangers were selling virtual assets that they obtained from their own involvement in other criminal activities, such as drug trafficking or computer hacking, or were otherwise knowingly facilitating the criminal activities of others.

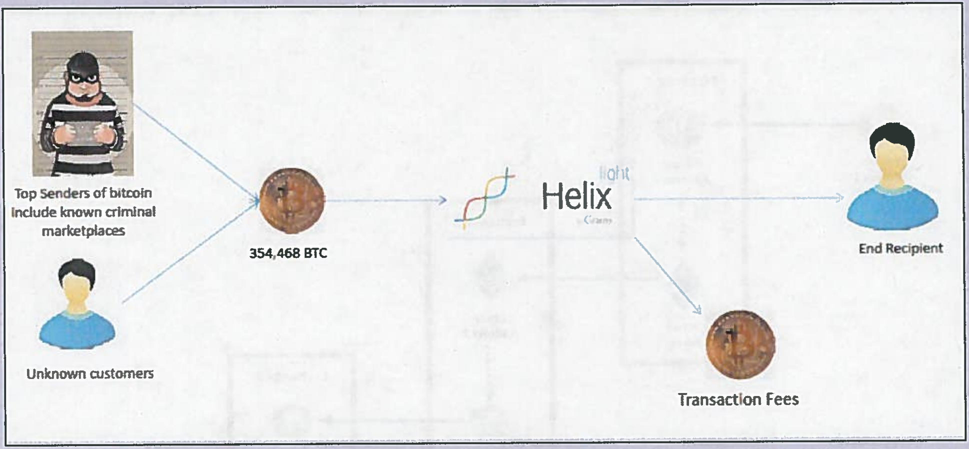
As discussed above, the Department has a broad range of legal authorities for investigating and prosecuting individuals who misuse cryptocurrency for criminal purposes. To that end, the Department is committed to an appropriate all-tools approach to dealing with cryptocurrency-related crime. The Department will continue

HELIX

On February 13, 2020, the Department of Justice announced the indictment and arrest of the alleged administrator of Helix, a darknet cryptocurrency laundering service. According to the indictment, Helix functioned as a bitcoin "mixer" or "tumbler," allowing customers to send bitcoin to designated recipients in a manner that was designed to conceal their source or owner.

The service's administrator is alleged to have advertised Helix to customers on the darknet as a way to conceal transactions from law enforcement. The indictment charges Helix with laundering over $300 million of bitcoin, which allegedly represented the proceeds of illicit narcotics sales and other criminal transactions.[158]

Figure 16: Helix Allegedly "Tumbled" a Large Volume of Bitcoin, Charging a Fee for Each Transaction



Helix allegedly received more than 354,468 bitcoin between the site's launch in June 2014 and December 2017, valued at approximately $311 million in U.S. dollars at the time of the transactions.

Figure 14: Example of a Criminal "Mixing" Enterprise

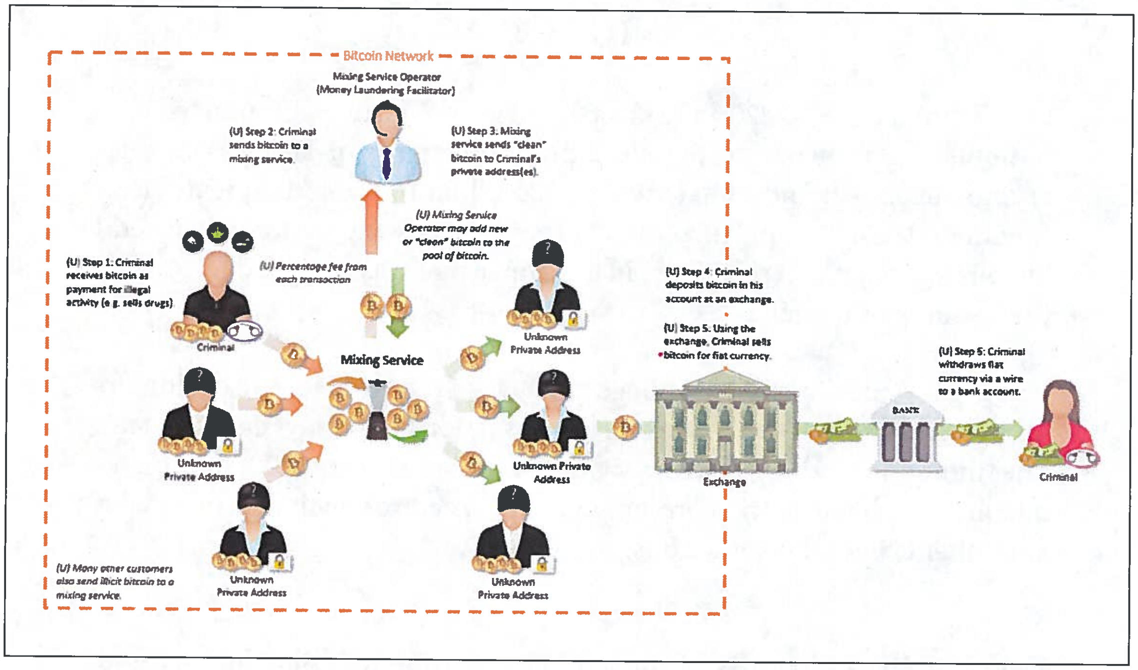
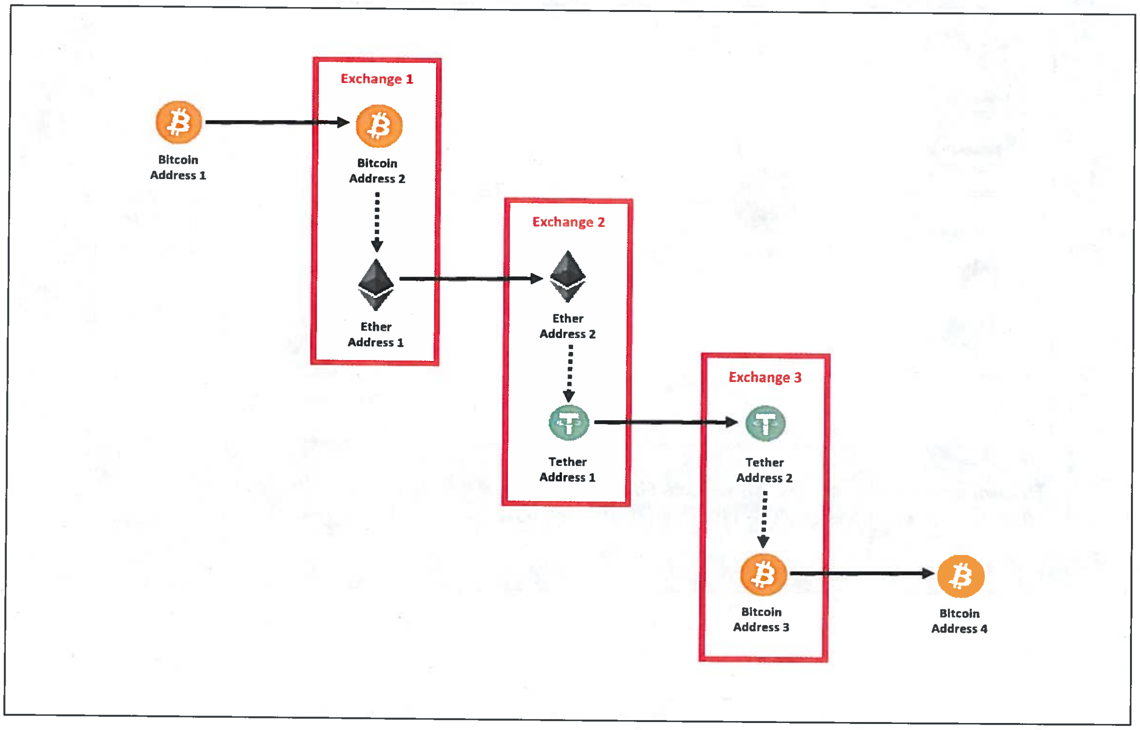

Bitcoin Network
Mixing Service Operator
(Money Laundering Facilitator)
(U) Step 2: Criminal sends bitcoin to a mixing service.
(U) Step 3: Mixing service sends "clean" bitcoin to Criminal's private address(es).
(U) Mixing Service Operator may add new or "clean" bitcoin to the pool of bitcoin.
(U) Step 1: Criminal receives bitcoin as payment for illegal activity (e.g. sells drugs)
(U) Percentage fee from each transaction
Criminal
Mixing Service
Unknown Private Address
Unknown Private Address
Unknown Private Address
Unknown Private Address
Unknown Private Address
(U) Step 4: Criminal deposits bitcoin in his account at an exchange.
(U) Step 5: Using the exchange, Criminal sells bitcoin for fiat currency.
(U) Step 5: Criminal withdraws fiat currency via a wire to a bank account.
BANK
Exchange
Criminal
(U) Many other customers also send illicit bitcoin to a mixing service.

Figure 15: Illustration of "Chain Hopping"



or authorized to do business as a casino in the United States by a federal, State, or tribal authority.[157] Casinos that do not meet this criterion are considered MSBs. Whether regulated as casinos or MSBs, these gambling businesses are subject to the BSA and its KYC record keeping and reporting requirements. Traditional brick-and-mortar casinos generally do not accept bitcoin or other cryptocurrencies; however, online gambling sites increasingly do accept cryptocurrencies. Online casinos that provide gambling services are also MSBs and must comply with applicable money transmission regulations. Although many do not have a known physical location, they still are required to report suspicious transactions to FinCEN if they offer services to U.S. customers.

Anonymity enhanced cryptocurrencies. The acceptance of anonymity enhanced cryptocurrencies or "AECs"—such as Monero, Dash, and Zcash—by MSBs and darknet marketplaces has increased the use of this type of virtual currency. As discussed above, because AECs use non-public or private blockchains, use of these cryptocurrencies may undermine the AML/CFT controls used to detect suspicious activity by MSBs and other financial institutions, and may limit or even negate a business's ability to conduct AML/CFT checks on customer activity and to satisfy BSA requirements. Some AECs, however, offer features, such as public view keys, that potentially can facilitate the fulfillment of AML/CFT obligations, depending upon the implementation of such features.

The Department considers the use of AECs to be a high-risk activity that is indicative of possible criminal conduct. In most circumstances, the Department does not liquidate seized or forfeited AECs, as doing so allows them to re-enter the stream of commerce for potential future criminal use. Companies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity, and should evaluate whether it is possible to adopt appropriate AML/CFT measures to address such risks.

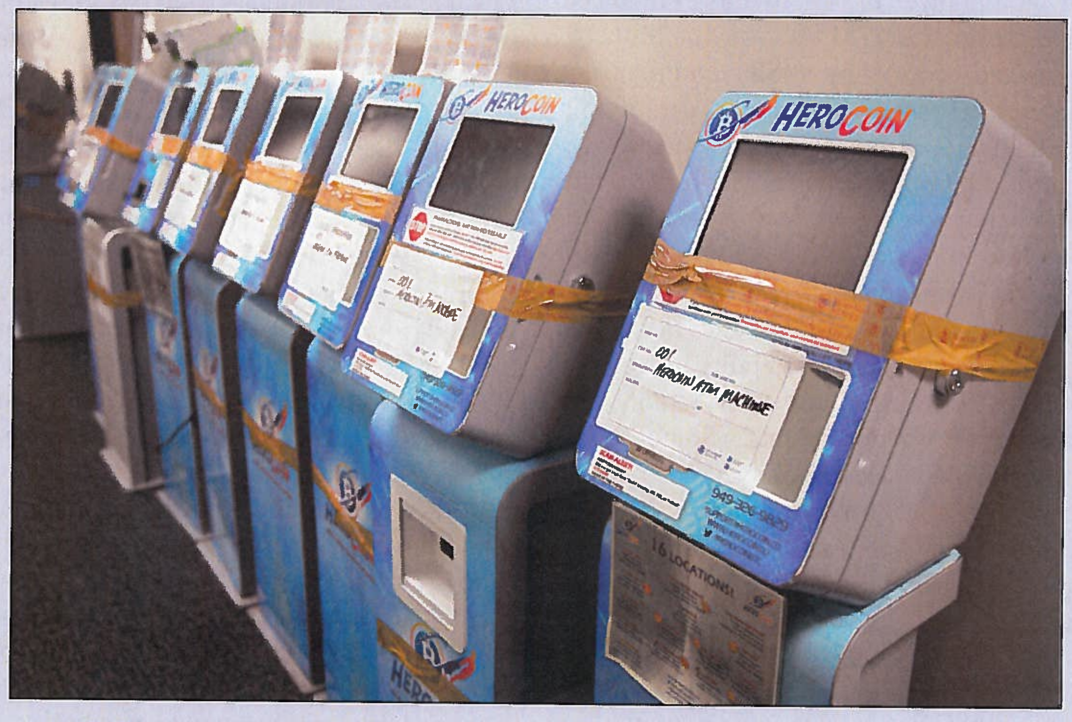
AECs are often exchanged for other virtual assets like bitcoin, which may indicate a cross-virtual-asset layering technique for users attempting to conceal criminal behavior. This practice, which is commonly referred to as "chain hopping," is discussed further below.

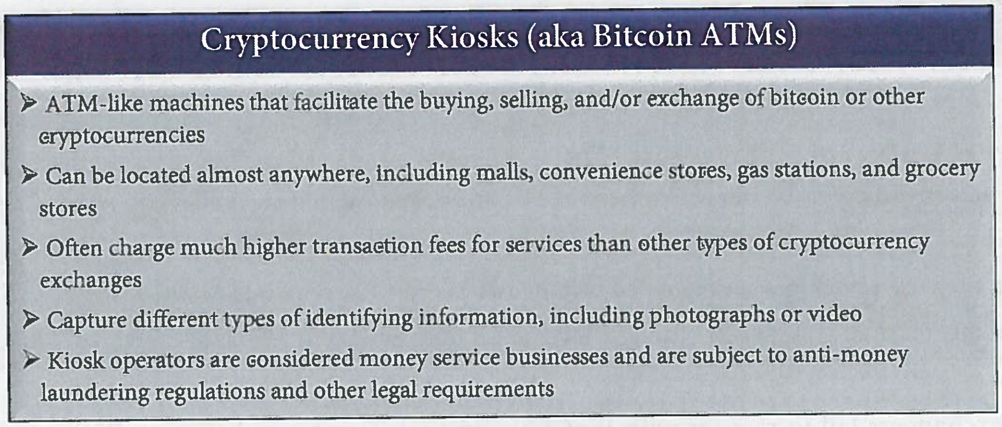
Mixers, tumblers, and chain hopping. "Mixers" and "tumblers" are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination. For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address. Websites or companies offering mixing or tumbling services are engaged in money transmission, and therefore are MSBs subject to the BSA and other similar international regulations. In addition to facing BSA liability for failing to register, conduct AML procedures, or collect customer identification, operators of these services can be criminally liable for money laundering because these mixers and tumblers are designed specifically to

Herocoin

On July 22, 2020, the Department of Justice announced that a California man agreed to plead guilty to operating an illegal virtual-currency money services business called Herocoin that exchanged up to $25 million—including proceeds of criminal activity—through in-person transactions and a network of Bitcoin ATM-type kiosks. The kiosks were installed in malls, gas stations, and convenience stores throughout California, and allowed customers to exchange cash for bitcoin and vice versa. In his plea agreement, the defendant admitted that he intentionally failed to register Herocoin with FinCEN, and failed to implement an effective anti-money laundering program; file currency transaction reports for exchanges in excess of $10,000; conduct due diligence on customers; or file suspicious activity reports. With respect to the Bitcoin ATM network, the defendant also admitted that he failed to implement a program to obtain identifications for customers conducting multiple transactions of up to $3,000 or verify that any identification provided actually reflected the person conducting the transaction. After pleading guilty, the defendant will face a statutory maximum sentence of 30 years in federal prison, and will forfeit cash, cryptocurrency, and 17 Bitcoin ATMs.[156]

Figure 13: Image of Cryptocurrency Kiosks Seized in the Herocoin Case





Cryptocurrency Kiosks (aka Bitcoin ATMs)

- ATM-like machines that facilitate the buying, selling, and/or exchange of bitcoin or other cryptocurrencies
- Can be located almost anywhere, including malls, convenience stores, gas stations, and grocery stores
- Often charge much higher transaction fees for services than other types of cryptocurrency exchanges
- Capture different types of identifying information, including photographs or video
- Kiosk operators are considered money service businesses and are subject to anti-money laundering regulations and other legal requirements

Cryptocurrency kiosk operators are considered MSBs in the United States. Accordingly, they are subject to the BSA and must register with FinCEN and follow all applicable money transmission requirements, including collecting and maintaining KYC data on their clients,[155] reporting suspicious transactions to FinCEN, filing currency transaction reports for fiat transactions of $10,000 or more in cash, and maintaining an effective AML/CFT program. While some operators comply with these requirements, many kiosks are not BSA-compliant and fail to collect required customer and transaction information. Indeed, investigators have linked such kiosks to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed virtual asset exchangers.

Virtual currency casinos. The rising popularity of virtual assets has led to the growth of virtual-currency-based "casinos" that facilitate various forms of betting denominated in bitcoin and other virtual currencies. Under current law, a casino that has gross annual gaming revenue in excess of $1 million must be duly licensed

Cryptocurrency Exchanges

- Allow users to buy and sell cryptocurrencies
- Serve as a conduit to the traditional financial system
- Can convert cryptocurrency to other virtual currencies or to fiat currency
- Global entities that can move money in seconds, not days
- In the U.S., exchanges are regulated by FinCEN as money service businesses
- In the international space, exchanges are subject to inconsistent regulatory regimes

P2P exchangers fail to register with FinCEN as MSBs or to comply with BSA obligations, and some even conduct transactions without requiring any form of identification from the customer.

P2P exchangers usually charge substantially higher percentage rates or fees—or use less favorable exchange rates—than registered exchanges. They often will accept a wide variety of payment methods, including payments of fiat currency in person or through the mail, deposits into bank accounts, Western Union or MoneyGram transfers, or payments in gift cards or stored value cards. P2P exchangers generally find their customers through word of mouth, open source websites such as Craigslist, or online exchange platforms.

P2P exchangers commonly use online exchange platforms or websites that allow users to trade virtual assets directly with one another and without a central operator. Nonetheless, when engaging in the transmission of virtual assets, these platforms must comply with BSA requirements. Although many P2P exchange platforms offer services similar to those offered by centralized virtual asset exchanges, P2P exchange platforms provide opportunities for cross-platform trading of cryptocurrency without the use of traditional financial institutions. Furthermore, unlike centralized virtual asset exchanges, P2P exchange platforms may operate without an intermediary that will accept and transmit virtual assets in exchange for fiat or another type of virtual asset, or that will collect customer identification information. Individual exchangers—as well as platforms and websites—that fail to collect and maintain customer or transactional data or maintain an effective AML/CFT program may be subject to civil and criminal penalties.[154]

Cryptocurrency kiosks. Cryptocurrency kiosks, which are commonly referred to as "Bitcoin ATMs," are stand-alone machines that allow users to convert fiat currency to and from bitcoin and other cryptocurrencies. With these machines, cryptocurrency can be bought or sold directly using a customer's mobile device or delivered in the form of a paper wallet. Thus, cryptocurrency kiosks offer an easy-to-use physical access point for virtual asset exchange.

III. Ongoing Challenges and Future Strategies

Parts I and II of this Framework discussed some of the serious public safety challenges posed by the misuse of cryptocurrency, and the legal and regulatory authorities the Department of Justice and its partners have used to address those challenges. This final Part explores the obligations of certain business and other entities that are particularly susceptible to abuse in the cryptocurrency space, and describes the Department's ongoing strategies for addressing these emerging threats to the safe and effective operation of the cryptocurrency marketplace.

A. Business Models and Activities That May Facilitate Criminal Activity

As described above, certain MSBs and other types of VASPs play a key role in the cryptocurrency ecosystem. Given their potential to facilitate criminal activity, these entities have a heightened responsibility to safeguard their platforms and businesses from exploitation by nefarious actors and to ensure that customer data is protected and secured. Moreover, the proper collection and maintenance of customer and transactional information by MSBs and other financial institutions pursuant to the BSA is crucial to the Department's ability to identify illicit actors, investigate criminal activity, and obtain evidence necessary for prosecutions. Key industry participants bearing these responsibilities include not only conventional virtual asset exchanges and brokers, but also peer-to-peer exchangers, kiosk operators, and online casinos, as discussed further below. Unfortunately, many entities in these new and growing sectors often fail to comply, in whole or in part, with the BSA and other legal requirements, thereby threatening the Department's investigative abilities and undermining public safety.

Cryptocurrency exchanges. Companies and individuals that offer cryptocurrency and other virtual asset exchange services to the public are commonly referred to as "exchanges" and "exchangers." Even exchanges that do not accept fiat currency and operate only with cryptocurrency are obliged to follow FinCEN record keeping and reporting requirements, as the applicable regulations cover transfers of value and are not specific to fiat transactions. Moreover, all entities, including foreign-located exchanges, that do business wholly or in substantial part within the United States, such as by servicing U.S. customers, must also register with FinCEN and have an agent physically present in the United States for BSA reporting and for accepting service of process.[152]

Peer-to-peer exchangers and platforms. Individuals seeking to buy or sell cryptocurrency other than through registered or licensed exchanges and financial institutions frequently turn to networks of individuals commonly referred to as peer-to-peer ("P2P") exchangers or traders. As individuals who facilitate transfers of value for the public, including the buying and selling of cryptocurrency, P2P exchangers are considered MSBs and are subject to FinCEN record keeping and reporting requirements.[153] In practice, however, many commitment to addressing illicit finance threats involving virtual assets. Under the leadership of the United States, which held the FATF presidency at the time, the FATF in October 2018 updated its standards to clarify their application to virtual asset activities by amending "Recommendation 15" and adding two new glossary definitions—"virtual asset" and "virtual asset service provider." Recommendation 15, which covers new technologies, states:

> To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.[149]

On June 21, 2019, the FATF adopted and issued a revised Interpretive Note to Recommendation 15 ("INR. 15") that further clarifies and expands upon the FATF's amendments to the standards relating to virtual assets, and describes how countries and obliged entities must comply with the relevant Recommendations to prevent the misuse of virtual assets for money laundering, terrorist financing, and proliferation.[150] Along with updated and expanded guidance aimed at assisting international jurisdictions and the private sector in implementing a risk-based approach to virtual assets and VASPs, INR. 15 requires countries to ensure that VASPs assess and mitigate their money laundering and terrorist financing risks, and implement the full range of AML/CFT preventive measures under the Recommendations—just like other entities subject to AML/CFT regulation. These measures include customer due diligence, record keeping, suspicious transaction reporting, and screening of transactions for compliance with targeted financial sanctions, among others.[151]

Interaction with the Department of Justice. The United States is a founding member of the FATF and, while holding the FATF presidency from July 2018 through June 2019, made it a priority to regulate VASPs for AML/CFT. The U.S. delegation to the FATF is led by the Department of the Treasury's Office of Terrorist Financing and Financial Crimes, and includes the Department of Justice as a key interagency partner. The delegation urged that all FATF Recommendations broadly apply to VASPs and virtual asset financial activities, which resulted in the successful adoption of the amendments to Recommendation 15 along with the Interpretive Note and guidance discussed above. Department of Justice attorneys provided significant contributions to the drafting and adoption process for these important changes to the FATF standards. The FATF also pursues ongoing work on trends in AML/CFT risk related to virtual assets, such as publicly identifying red flags in virtual asset financial activity, and issuing reports that provide case studies drawn from all over the FATF's global network. The Department of Justice has been an integral partner in this effort, providing analysis and case examples for the U.S. delegation.

C. International Regulation

As discussed further below, the lack of consistent international regulation and enforcement of anti-money laundering and combating the financing of terrorism standards applicable to virtual asset entities represents a major challenge. There are, however, important organizations in the international regulatory space, especially the global standard-setter for AML/CFT standards—the Financial Action Task Force ("FATF").[147]

The Financial Action Task Force. The FATF is an intergovernmental organization that was founded in 1989 on the initiative of the G7 by the ministers of its member jurisdictions.[148] Its objectives are to set standards and to promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system. As a standard-setting and policy-making body, the FATF works to generate the technical understanding and necessary political will to bring about national legislative and regulatory reforms, which are intended to be harmonized across jurisdictions to the greatest extent possible.

The FATF reviews money laundering and terrorist financing techniques and countermeasures; provides a forum for exchange of best practices; highlights areas of common concern; and promotes and monitors the progress of its members in adopting and implementing regulatory measures globally. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities as part of its peer review process with the aim of protecting the international financial system from misuse, as well as creating standards for national best practices.

The FATF Recommendations and Virtual Asset Guidance. The FATF has developed a series of "Recommendations" that are recognized as the international standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. FATF member countries are responsible for implementing the standards at the national level for compliance by the private sector. This provides the foundation for a coordinated international response aimed at confronting these threats to the integrity of the global financial system.

In 2014, the FATF recognized the need to bring virtual-asset-related activities within its scope, and in 2015 issued global guidance as part of a staged approach to addressing the money-laundering and terrorist-financing risks associated with virtual asset payment products and services. In July 2018, the FATF published a report at the G20 Finance Ministers and Central Bank Governors' meeting outlining the FATF's

On October 9, 2019, the IRS issued additional guidance and FAQs for taxpayers who engage in virtual currency transactions, in an effort to help them better understand their reporting obligations. The guidance addresses the tax treatment of "hard forks," which occur when a cryptocurrency undergoes a protocol change resulting in a new distributed ledger and a new cryptocurrency, in addition to the original distributed ledger.[139] The FAQs also address more basic questions about, for example, calculating gains or losses when selling or exchanging virtual currency for real currency or property; whether virtual currency paid by an employer for services constitutes taxable income; and maintaining records of transactions in virtual currency.[140] On December 31, 2019, the IRS issued additional FAQs for taxpayers relating to charitable donations in virtual currency.[141]

7. State Authorities

State attorneys general, securities regulators, and departments of financial services are responsible for protecting the investing public in their respective States by, for example, licensing securities firms and investment professionals (such as broker-dealers and investment advisers); registering certain securities offerings; reviewing financial offerings by companies; auditing sales practices and record keeping; promoting investor education; and enforcing State securities and banking laws.[142] Many State authorities are actively monitoring, supervising, or investigating virtual asset activities within their jurisdictions, particularly those involving the issuance or sale of ICOs and other investment products.

For example, on May 21, 2018, the North American Securities Administrators Association ("NASAA")[143] announced a coordinated series of enforcement actions by State and provincial securities regulators in the United States and Canada to crack down on fraudulent ICOs and cryptocurrency-related investment products, as well as on the fraudsters behind them. More than 40 jurisdictions throughout North America participated in "Operation Cryptosweep," which resulted in nearly 70 inquiries and investigations and 35 pending or completed enforcement actions related to ICOs or cryptocurrencies.[144]

The State of New York has been one of the more proactive States seeking to regulate and gather information in the virtual asset and ICO space. New York State officials are conducting a Virtual Markets Integrity Initiative, which is a fact-finding inquiry into the policies and practices of platforms used by consumers to trade cryptocurrencies.[145]As part of that initiative, on April 17, 2018, the New York Attorney General's Office sent letters to thirteen entities identified as "major virtual currency trading platforms" or "exchanges," requesting disclosures about their operations, use of bots, conflicts of interest, outages, and other issues.[146] The letters also requested information on the covered entities' operations, internal controls, and safeguards to protect customer assets as part of a broader effort to protect cryptocurrency investors and consumers.

16, 2018, filed a complaint in federal court in New York charging Blake Harrison Kantor and Nathan Mullins, as well as several entities located in the United States and abroad, with operating a fraudulent scheme covering binary options and a virtual currency known as ATM Coin.[133] The CFTC's complaint alleged that, since at least April 2014, the defendants solicited potential customers through emails, phone calls, and a website to purchase illegal off-exchange binary options. Additionally, the defendants falsely claimed that customers' accounts would generate significant profits based upon Kantor's purported profitable trading history, and allegedly misappropriated a substantial amount of the customer funds for personal use. The defendants were alleged to have sought to cover up their misappropriation by inviting customers to transfer their binary options account balances into ATM Coin. Some customers agreed to transfer their funds into ATM Coin, and at least one customer sent additional money to the defendants to purchase additional ATM Coin. The defendants then allegedly misrepresented to customers that their ATM Coin holdings were worth substantial sums of money. On October 23, 2019, a federal court entered an order finding that the defendants had committed fraud and had misappropriated client funds, and requiring them to pay a total of $4.25 million.[134] In a parallel action, the United States Attorney for the Eastern District of New York filed a criminal indictment charging Kantor with fraud, obstruction, and making false statements. He pleaded guilty to the wire fraud conspiracy and obstruction charges, and was sentenced on July 1, 2019, to 86 months' imprisonment.[135]

6. The IRS and Tax Enforcement

The Internal Revenue Service ("IRS") treats virtual currency as property for U.S. federal tax purposes, which means that the general tax principles that apply to property transactions also apply to virtual currency transactions.[136] Income, including capital gains, from virtual currency transactions is taxable, and virtual currency transactions themselves must be reported on a taxpayer's income tax return.[137]

In addition, wages paid in virtual currency to employees are taxable, reportable on a Form W-2, and subject to withholding and payroll taxes. Businesses that receive payments for goods or services in virtual currency are required to include such payments in their gross income. The Department of Justice's Tax Division and U.S. Attorney's Offices around the country may pursue tax related prosecutions in cases involving the failure to report income from virtual currency. The Department of Justice also works with the IRS to support its enforcement and compliance efforts relating to virtual currency, including enforcing summonses issued to taxpayers and third parties, as well as assisting in "John Doe" summons matters.[138]

could offer consumers FDIC insured accounts and traditional banking services, in addition to cryptocurrency services. These statements were false. Rice, who had converted investor funds for his own personal use, also claimed falsely that the ICO had raised $600 million in a matter of weeks.[119] On March 20, 2019, Rice pleaded guilty in the criminal proceedings to one count of securities fraud, in violation of 15 U.S.C. §§ 78j and 78ff. In the SEC's civil action, Rice and AriseBank COO Stanley Ford agreed to pay nearly $2.7 million in disgorgements, interest, and penalties, without admitting or denying the allegations. Both Rice and Ford are permanently enjoined from violating the antifraud and registration provisions of the federal securities laws, from ever serving as officers or directors of public companies, and from participating in issuances, offers, or sales of digital securities.[120]

5. The Commodity Futures Trading Commission

Statutory authority. Like the SEC, the Commodity Futures Trading Commission ("CFTC") has statutory authority with respect to certain aspects and uses of virtual assets. Under the Commodity Exchange Act ("CEA"),[121] the CFTC has oversight over derivatives contracts, including futures, options, and swaps,[122] that involve a commodity. The CEA defines "commodity" to include agricultural products, "all other goods and articles," and "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[123] The CFTC has concluded that certain virtual currencies are "commodities" under the CEA.[124] In addition, multiple federal courts have held that virtual currencies fall within the CEA's definition of commodity.[125]

The CFTC's jurisdiction is implicated when a virtual currency is the underlying asset in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. "Beyond instances of fraud or manipulation, the CFTC generally does not oversee 'spot' or cash market exchanges and transactions involving virtual currencies which do not utilize margin, leverage, or financing."[126] The CFTC has taken action against unregistered bitcoin futures exchanges and firms illegally offering margined or financed retail virtual currency transactions;[127] enforced laws prohibiting fictitious trades on a derivatives platform[128] and laws requiring firms to implement adequate anti-money laundering procedures;[129] issued interpretative guidance concerning whether "actual delivery" has occurred in the context of retail commodity transactions in virtual currencies;[130] issued warnings about valuations and volatility in spot virtual currency markets;[131] and addressed numerous virtual currency Ponzi schemes.[132]

Interaction with the Department of Justice. In a case involving parallel action by the Department of Justice, the CFTC on April

TON Issuer Inc. began raising capital in January 2018 to finance the companies' business, including the development of their own blockchain, the 'Telegram Open Network' or 'TON Blockchain,' as well as the mobile messaging application Telegram Messenger."[110] As part of their plan to raise funds, the entities sold "approximately 2.9 billion digital tokens called 'Grams' at discounted prices to 171 initial purchasers worldwide, including more than 1 billion Grams to 39 U.S. purchasers."[111] The SEC's complaint alleged that Telegram and TON Issuer failed to register their offers and sales of the new "Grams" cryptocurrency, in violation of the registration provisions of the Securities Act of 1933.[112]

In March 2020, a federal judge granted the SEC a preliminary injunction, ruling that the agency had shown "a substantial likelihood of success in proving that the contracts and understandings at issue, including the sale of 2.9 billion Grams to 175 purchasers in exchange for $1.7 billion, are part of a larger scheme to distribute those Grams into a secondary public market, which would be supported by Telegram's ongoing efforts."[113]Accordingly, the court concluded that, on the facts before it, "the resale of Grams into the secondary public market would be an integral part of the sale of securities without a required registration statement."[114] Three months later, the court approved a settlement between the parties, whereby Telegram and its subsidiary agreed not to appeal the court's ruling and consented to the court's judgment without admitting or denying the SEC's allegations. The court ordered Telegram to disgorge $1,224,000,000 in ill-gotten gains from the sale of Grams, with credit for the amounts paid back to initial purchasers of Grams, and also ordered Telegram to pay a civil penalty of $18,500,000.[115]

The SEC's landmark Telegram case underscores why companies and individuals working and innovating in the digital assets space should ensure—prior to offering or selling—that their activities will meet all applicable requirements under the federal securities laws.[116] Of course, in cases involving outright fraud, bad actors face not only a variety of potential civil securities law violations, but also potential criminal prosecution for fraud or theft.[117]

Interaction with the Department of Justice. The SEC works closely with the Department of Justice in cases involving criminal violations of the federal securities laws, including cases related to ICOs. As just one example, on January 25, 2018, the SEC filed a civil complaint in federal court in Texas seeking to halt an allegedly fraudulent ICO by AriseBank. The same week, the FBI and the SEC coordinated the timing of a search at the temporary residence of the ICO issuer with the execution of a freeze order by a receiver in the SEC's civil action, resulting in the recovery of cryptocurrency for the victim investors.[118] Subsequently, in the Department of Justice's related criminal case, a federal grand jury in Dallas charged AriseBank CEO Jared Rice, Sr., on November 20, 2018, for defrauding investors out of $4 million worth of cryptocurrency assets. The Department's investigation revealed that Rice claimed in connection with the ICO that a cryptocurrency token called "AriseCoin" via a blockchain network, typically do not provide traditional "shares" in the issuing company. Instead, they might purport to grant access to a good or service, to the right to a share in the relevant project's earnings, or to a potential increase in value based on the project's success.[99] Recognizing the securities law implications for technological developments like blockchain and distributed ledger technologies, digital assets (including cryptocurrency), digital asset securities, and other digital instruments, the SEC has devoted substantial resources to this area.[100]

In 2017, the SEC issued an investigative report cautioning the public that offers and sales of digital assets—including through ICOs and token sales—by "virtual" organizations may be subject to the requirements of the federal securities laws, which include registration and disclosure mandates.[101] As the SEC explained, "[w]hether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[102] To protect investors and the public, the SEC has summarily suspended, for 10 business days, the trading of securities of more than a dozen issuers when there were concerns about the accuracy and adequacy of information in the marketplace regarding securities offered or sold through ICOs or coin- or token- related news.[103] The SEC also has warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs. And the SEC has filed ICO-related civil enforcement actions against individuals violating the securities laws or engaging in fraudulent schemes.[104]

On April 3, 2019, the SEC Staff released a framework for analyzing whether "a digital asset is offered or sold as an investment contract, and, therefore, is a security" under the federal securities laws.[105] The term "security" includes an "investment contract," as well as other instruments such as stocks, bonds, and transferable shares. Under the so-called "*Howey* test," derived from the Supreme Court's seminal 1946 decision in *Securities and Exchange Commission v. W. J. Howey Co.*, an "investment contract" exists if there is an investment of money in a common enterprise with an expectation of profits derived from the efforts of others.[106] The framework is careful to note that, in the digital asset context, as with all other assets, this analysis does not depend only on the "form and terms" of the asset itself, "but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold."[107] The SEC encourages individuals and entities in the digital asset marketplace to engage proactively with SEC staff as the marketplace continues to develop.[108]

A high-profile action brought by the SEC in October 2019 highlights the need for individuals and entities in the global digital asset marketplace to ensure they are in compliance with U.S. federal securities laws. That month, the SEC sought and received a temporary restraining order against two offshore entities conducting an unregistered, ongoing digital token offering both within the United States and overseas that had raised more than $1.7 billion of investor funds.[109] According to the SEC's complaint, "Telegram Group Inc. and its wholly-owned subsidiary

3. Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency ("OCC") is an independent branch of the U.S. Department of the Treasury that charters, regulates, and supervises national banks and federal savings associations. OCC issues rules and regulations for banks and can "impos[e] corrective measures, when necessary, on OCC-governed banks that do not comply with laws and regulations or that otherwise engage in unsafe or unsound practices."[93] On July 22, 2020, OCC published an Interpretive Letter to clarify the authority of national banks and federal savings associations to provide cryptocurrency custody services for their customers.[94] The Letter concludes that such services, which include "holding the unique cryptographic keys associated with cryptocurrency," are a permissible modern form of traditional bank activities.[95] It also stressed OCC's position that banks can provide their services to lawful cryptocurrency businesses "so long as they effectively manage the risks and comply with applicable law."[96]

Earlier in 2020, OCC entered into a cease-and-desist consent order with M.Y. Safra Bank, after alleging that the bank violated the BSA's requirements for establishing an adequate AML program and failed to investigate suspicious transactions and to timely file SARs. Among other things, OCC's investigation revealed that the bank failed to sufficiently consider AML risks and implement appropriate risk controls when opening accounts for customers that operated virtual-currency money services businesses.[97] Pursuant to the consent order, the bank must adopt numerous improvements to its risk profile, system of internal controls, customer due diligence operation, and BSA audit program.

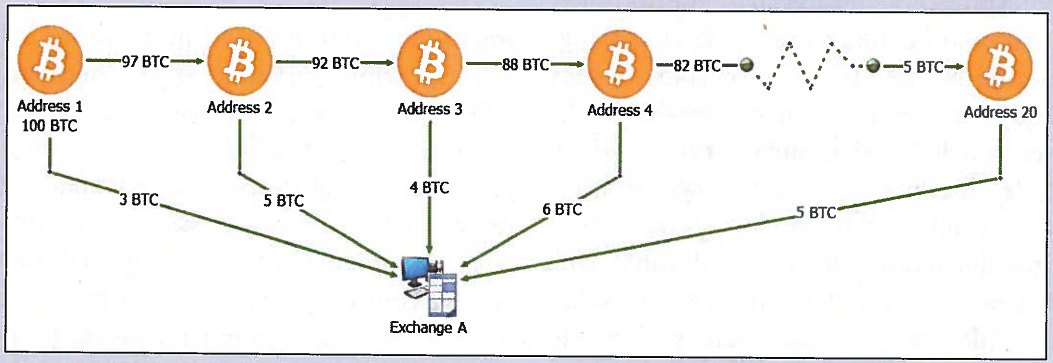
4. The Securities and Exchange Commission

Regulatory authority. The mission of the U.S. Securities and Exchange Commission ("SEC") is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation. Of particular relevance to the SEC's mission in the virtual currency context is the rapid growth of the "initial coin offerings" ("ICOs") market and its widespread promotion as a means for new investment opportunity, which has provided fertile ground for malicious actors to swindle investors. ICOs (which are also known as "token sales"[98]) are a means companies have used to raise capital by offering and selling digital tokens to potential investors in exchange for funding a certain project or platform. The tokens purchased by an investor in an ICO, which are distributed

CASE STUDY: THE NORTH KOREAN HACKS

As discussed in the text, on the same day in March 2020 that OFAC announced sanctions, the Department of Justice announced criminal charges against two Chinese nationals for laundering over $100 million worth of cryptocurrency that the defendants allegedly obtained from North Korean actors who had hacked cryptocurrency exchanges.[88] In March and August 2020, the Department also announced complaints seeing the civil forfeiture of hundreds of virtual currency accounts associated with related North Korean hacks and subsequent money laundering conspiracies.[89] The investigations into these criminal schemes revealed highly sophisticated money-laundering techniques. For example, criminal actors allegedly laundered the funds illicitly obtained from the hacks through several intermediary addresses and other virtual currency exchanges. On several occasions, the actors allegedly used the chain-hopping technique in an attempt to obfuscate the transaction path by converting the stolen cryptocurrency into BTC, Tether, or other forms of cryptocurrency.[90] The actors also allegedly used "peel chains" to conceal their activity, whereby "a large amount of [cryptocurrency] sitting at one address is sent through a series of transactions in which a slightly smaller amount of [cryptocurrency] is transferred to a new address each time."[91]

Figure 12: Depiction of a Simple "Peel Chain"



This chart depicts a hypothetical "peel chain" where a subject deposits 100 total bitcoin into an exchange. The subject forwards the bitcoin through a series of 20 "peels" in inconsistent amounts in an attempt to make the underlying transaction difficult to track. In practice, sophisticated cybercriminals often use hundreds of transactions to obscure the path of funds.[92]

The successful investigations into the North Korean cryptocurrency hacks and subsequent money-laundering scheme—and the coordinated actions between OFAC and the Department of Justice—demonstrate the importance of interagency coordination in addressing threats within the virtual currency space.

In August 2019, OFAC designated three Chinese nationals, one Chinese drug trafficking organization, and one Chinese pharmaceutical company for their involvement with fentanyl manufacturing and trafficking pursuant to the Foreign Narcotics Kingpin Designation Act ("Kingpin Act"). OFAC identified cryptocurrency addresses associated with two drug traffickers to maximize disruption of their financial dealings.[79] OFAC closely coordinated these designations with the Department of Justice. Previously, in 2017, the Department of Justice indicted one of the Chinese nationals for his role as a manufacturer and distributor of fentanyl and other opiate substances.[80] And in August 2018, the Department of Justice charged two of the Chinese nationals with operating a conspiracy that manufactured and shipped deadly fentanyl analogues and 250 other drugs to at least 25 countries and 37 states.[81]

In September 2020, OFAC designated three Russian nationals for having acted or purported to act for or on behalf of, directly or indirectly, the Internet Research Agency ("IRA"), an entity previously designated for its involvement with election interference activities, pursuant to EO 13694, as amended by EO 13757, and EO 13848. The IRA uses cryptocurrency to fund activities in furtherance of ongoing malign influence operations around the world. OFAC identified digital currency addresses for two of these Russian nationals.[82] Concurrently, the Department of Justice filed a criminal complaint charging one of the Russian nationals for his alleged role in a conspiracy to use the stolen identities of real U.S. persons to open fraudulent accounts at banking and cryptocurrency exchanges.[83]

Earlier, on March 2, 2020, OFAC announced sanctions pursuant to EOs 13722 and 13694, as amended, against two Chinese nationals who are alleged to have laundered over $100 million worth of cryptocurrency stolen from cryptocurrency exchanges by North Korean actors. This theft is another example of North Korea's cyber heist program (see page 28), which trains actors to target and launder stolen funds—including large amounts of cryptocurrency—from financial institutions.[84] The two sanctioned individuals allegedly received the stolen cryptocurrency from accounts controlled by North Korean actors and subsequently transferred the funds among cryptocurrency addresses to obfuscate their origin. As a result of OFAC's action, "all property and interests in property of these individuals that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC."[85] On the same day that OFAC announced these sanctions, the Department of Justice announced criminal charges against the two individuals for money laundering conspiracy and for operating an unlicensed money transmitting business, as well as the seizure of the illicit funds.[86] Subsequently, on August 27, 2020, the Department filed a complaint seeking civil forfeiture of 280 additional virtual currency addresses and accounts linked to the hacks.[87] The coordinated actions by OFAC and the Department of Justice followed a comprehensive investigation led by the FBI, IRS–Criminal Investigation, and Homeland Security Investigations, further demonstrating the importance of cooperation among investigatory agencies.

2. Office of Foreign Assets Control

Regulatory authority. Virtual assets move globally, and in some instances they move to entities or jurisdictions subject to economic sanctions administered by the U.S. Department of the Treasury. The Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces economic and trade sanctions against targeted foreign countries and regimes; terrorist groups; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; those engaged in malicious cyber activities; and other entities that present threats to the national security, foreign policy, or economy of the United States based on U.S. foreign policy and national security goals.[69]

As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction—including firms that facilitate or engage in online commerce or process transactions using digital currency[70]—are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions (such as dealings with blocked persons or property) or in otherwise-prohibited trade or investment-related transactions.[71] Prohibited transactions generally also include those that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities.[72] In addition, persons who provide financial, material, or technological support for or to a designated person or entity, or certain malicious activities, may themselves be designated by OFAC under the relevant sanctions authority, or be criminally or civilly liable for violations of the Trading With the Enemies Act, the International Emergency Economic Powers Act, and other statutes.[73]

Interaction with the Department of Justice. On November 28, 2018, OFAC took its first virtual-asset-related action pursuant to the "cyber sanctions" authorized by Executive Order ("EO") 13694, as amended by EO 13757.[74] This action targeted two Iran based individuals who helped exchange bitcoin ransom payments into Iranian rial on behalf of malicious Iranian cyber actors involved with the SamSam ransomware scheme described above.[75] OFAC also identified two bitcoin addresses associated with these individuals that were connected to over 7,000 transactions worth millions of dollars.[76] By designating these malicious cyber actors, OFAC sought to "aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards," while also encouraging "virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services [to] harden their networks against [such] illicit schemes."[77] As described above, in a related move, the Department of Justice brought criminal charges against the two Iran-based individuals related to the 34-month-long international computer hacking and extortion scheme involving the use of SamSam ransomware against numerous U.S. computer networks.[78]

EXHIBIT 199

[redacted]

Harvard Law School Forum on Corporate Governance

An Introduction to Smart Contracts and Their Potential and Inherent Limitations

Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP, on Saturday, May 26, 2018

Tags: Blockchain, Contracts, Cybersecurity, Financial technology, Legal systems, Risk, Risk management
More from: Alex Lipton, Stuart Levi, Skadden

Editor's Note: Stuart D. Levi is a partner and Alex B. Lipton is an associate at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on their Skadden publication.

"Smart contracts" are a critical component of many platforms and applications being built using blockchain or distributed ledger technology. Below, we outline the background and functions of smart contracts, discuss whether they can be deemed enforceable legal agreements under contract law in the United States, and highlight certain legal and practical considerations that will need to be resolved before they can be broadly used in commercial contexts.

An Introduction to Smart Contracts

How Smart Contracts Function

"Smart contracts" is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. As discussed further below, the code can either be the sole manifestation of the agreement between the parties or might complement a traditional text-based contract and execute certain provisions, such as transferring funds from Party A to Party B. The code itself is replicated across multiple nodes of a blockchain and, therefore, benefits from the security, permanence and immutability that a blockchain offers. That replication also means that as each new block is added to the blockchain, the code is, in effect, executed. If the parties have indicated, by initiating a transaction, that certain parameters have been met, the code will execute the step triggered by those parameters. If no such transaction has been initiated, the code will not take any steps. Most smart contracts are written in one of the programming languages directly suited for such computer programs, such as Solidity.

At present, the input parameters and the execution steps for a smart contract need to be specific and objective. In other words, if "x" occurs, then execute step "y." Therefore, the actual tasks that smart contracts are performing are fairly rudimentary, such as automatically moving an amount of cryptocurrency from one party's wallet to another when certain criteria are satisfied. As the adoption of blockchain spreads, and as more assets are tokenized or go "on chain," smart contracts will become increasingly complex and capable of handling sophisticated transactions. Indeed, developers already are stringing together multiple transaction steps to form more complex smart contracts. Nonetheless, we are, at the very least, many years away from code being able to determine more subjective legal criteria, such as whether a party satisfied a commercially reasonable efforts standard or whether an indemnifications clause should be triggered and the indemnity paid.

Before a compiled smart contract actually can be executed on certain blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum blockchain, smart contracts are executed on the Ethereum Virtual Machine (EVM), and this payment, made through the ether cryptocurrency, is known as "gas." [1] The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to prevent overly complex or numerous smart contracts from overwhelming the EVM. [2]

[redacted]

Smart contracts are presently best suited to execute automatically two types of "transactions" found in many contracts: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied. In each case, human intervention, including through a trusted escrow holder or even the judicial system, is not required once the smart contract has been deployed and is operational, thereby reducing the execution and enforcement costs of the contracting process.

As just one example, smart contracts could eliminate the so-called procure-to-pay gaps. When a product arrives and is scanned at a warehouse, a smart contract could immediately trigger requests for the required approvals and, once obtained, immediately transfer funds from the buyer to the seller. Sellers would get paid faster and no longer need to engage in dunning, and buyers would reduce their account payable costs. This could impact working capital requirements and simplify finance operations for both parties. On the enforcement side, a smart contract could be programmed to shut off access to an internet-connected asset if a payment is not received. For example, access to certain content might automatically be denied if payment was not received.

Historical Background

The term "smart contract" was first introduced by computer scientist and cryptographer Nick Szabo some 20 years ago as a graduate student at University of Washington. According to Szabo:

> New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart," because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises. [3]

Szabo's use of quotes around the word "smart" when comparing smart contracts to paper-based contracts, and his eschewing of artificial intelligence are important. Smart contracts may be "smarter" than paper contracts because they automatically can execute certain pre-programmed steps, but they should not be seen as intelligent tools that can parse a contract's more subjective requirements. Indeed, the classic example of a smart contract offered by Szabo is a vending machine. Once a purchaser has satisfied the conditions of the "contract" (*i.e.*, inserting money into the machine) the machine automatically honors the terms of the unwritten agreement and delivers the snack.

Smart contracts today also find their origin in Ricardian Contracts, a concept published in 1996 by Ian Grigg and Gary Howland as part of their work on the Ricardo payment system to transfer assets. Grigg saw Ricardian Contracts as a bridge between text contracts and code that had the following parameters: a single document that "is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier." [4]

The Interplay With Traditional Text Agreements

One of the difficulties with discussing smart contracts is that the term is used to capture two very different paradigms. The first involves smart contracts that are created and deployed without any enforceable text-based contract behind them. For example, two parties reach an oral understanding as to the business relationship they want to capture and then directly reduce that understanding into executable code. We refer to these below as "code-only smart contracts." The second paradigm involves the use of smart contracts as vehicles to effectuate certain provisions of a traditional text-based contract, in which the text itself references the use of the smart contract to effectuate certain provisions. We refer to these as "ancillary smart contracts."

Are Smart Contracts Enforceable?

There is no federal contract law in the United States; rather, the enforceability and interpretation of contracts is determined at the state level. Thus, while certain core principles apply consistently across state lines, and there has been a drive to harmonize state laws by the National Conference of Commissioners on Uniform State Laws, any conclusions regarding smart contracts must be tempered by the reality that states may adopt different views.

A discussion regarding the enforceability of smart contracts must start with the fundamental distinction between an agreement and a "contract." States generally recognize that although two parties can enter into a variety of "agreements," a contract means that the agreement is legally binding and enforceable in a court of law. [5] In order to determine enforceability, state courts traditionally look to whether the common law requirements of offer, acceptance and consideration are satisfied. These basic requirements surely can be achieved through ancillary smart contracts. For example, an insurer might develop a flight insurance product that automatically provides the insured with a payout if a flight is delayed by more than two hours. [6] The key terms, such as delineating how the delay is calculated, can be set forth in a text-based contract, with the actual formation of the contract (payment of the premium) and the execution (automatic payout upon a verifiable delay) handled through an ancillary smart contract. Here, the insurer has made a definite offer for a flight insurance product that is accepted by the insured upon payment of the premium as consideration.

Although, today, certain contracts must be in writing, and additional formalities may be required such as those under the Uniform Commercial Code (UCC) and state statutes of frauds, [7] agreements do not always need to be in writing to be held enforceable. [8] Thus, many code-only smart contracts also will be enforceable under state laws governing contracts. Szabo's example of a vending machine is instructive in this regard. There, while the buyer has many implied rights, a contract was formed without any meaningful written terms other than a price display for each item. Thus, the fact that an agreement is rendered only in code, such as the case with code-only smart contracts, presents no particular barrier to contract formation outside the barriers imposed by the UCC and statutes of frauds. Indeed, a variety of laws and legal constructs have long considered the role of information technology in contract formation.

For example, the Uniform Electronic Transactions Act (UETA) which dates back to 1999 and forms the basis for state law in 47 states, provides that, with limited exceptions, electronic records, which include records created by computer programs, and electronic signatures (*i.e.*, digital signature using public key encryption technology) be given the same legal effect as their written counterparts. [9] UETA even goes so far as recognizing the validity of "electronic agents," which it defines as "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." [10] Under UETA, an electronic agent is "capable within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party," [11] arguably a prescient acknowledgment of smart contracts.

Similarly, the federal Electronic Signatures Recording Act (E-Sign Act) not only recognizes the validity of electronic signatures and electronic records in interstate commerce, but also provides that a contract or other record relating to a transaction "may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound." [12] The term "electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response." [13]

Though an understanding of the current legal framework is important to evaluating the enforceability of smart contracts today, those using smart contracts in the future may not need to rely on laws that pre-date the development of blockchain technology. Arizona and Nevada already have amended their respective state versions of UETA to explicitly incorporate blockchains and smart contracts. [14] The fact that these states have adopted decidedly different definitions of those critical terms suggests that as more states follow their lead, there may be increasing pressure to adopt unified definitions to reflect blockchain and smart contract developments.

Challenges With the Widespread Adoption of Smart Contracts

Given the existing legal frameworks for recognizing electronic contracts, it is quite likely that a court today would recognize the validity of code that executes provisions of a smart contract—what we have classified as ancillary smart contracts. There is also precedent to suggest that a code-only smart contract might enjoy similar legal protection. The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business. We set forth below certain of these challenges:

How Can Non-technical Parties Negotiate, Draft and Adjudicate Smart Contracts?

A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate. While some analogize this to hiring a lawyer to explain "the legalese" of a traditional text-based contract, the analogy is misplaced. Non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms. But a non-programmer would be at a total loss to understand even the most basic smart contract and is therefore significantly more beholden to an expert to explain what the contract "says."

To some extent, the inability of contracting parties to understand the smart contract code will not be a hindrance to entering into ancillary code agreements. This is because for many basic functions, text templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. For example, assume a simple smart contract function that extracts a late fee from a counterparty's wallet if a defined payment is not received by a specified date. The text template could prompt the parties to enter the amount of the expected payment, the due date and the amount of the late fee. However, a party may want to confirm that the underlying code actually will perform the functions specified in the text, and that there are no additional conditions or parameters—especially where the template disclaims any liability arising from the accuracy of the underlying code. This review will require a trusted third party with programming expertise.

In cases where such templates do not exist, and new code must be developed, the parties will need to communicate the intent of their agreement to a programmer. Simply handing that programmer a copy of the legal agreement would be inefficient since it would require the programmer to try and decipher a legal document. Parties relying on ancillary smart contracts therefore may need to draft a separate "term sheet" of functionality that the smart contract should perform and that can be provided to the programmer.

The parties also may want written representations from the programmer that the code performs as contemplated. The net result is that for customized arrangements that do not rely on an existing template, the parties may need to enter into a written agreement with the smart contract programmer, not unlike the contract that parties may enter into with a provider of services for Electronic Data Interchange (EDI) transactions today.

Insurance companies could also create policies to protect contracting parties from the risk that smart contract code does not perform the functions specified in the text of an agreement. Although the parties would also want to review (or have third parties review) the code, insurance can provide additional protection given that the parties might miss errors when reviewing the code. The parties would also take some additional comfort from the fact that the insurance company likely conducted its own code audit before agreeing to insure the code.

Code-only smart contracts used for business-to-consumer transactions could pose an additional set of issues that will need to be addressed. Courts are wary of enforcing agreements where the consumer did not receive adequate notice of the terms of the agreement, **[15]** and may be hesitant to enforce a smart contract where the consumer was not also provided with an underlying text agreement that included the complete terms.

Finally, as the validity or performance of smart contracts increasingly become adjudicated, courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Today, parties routinely use their own experts when technical issues are at the center of a dispute. While both federal courts and many state courts have the authority to appoint their own experts, they rarely exercise that authority. **[16]** That approach may need to change if the number of standard contract disputes that center on interpreting smart contract code increases.

Smart Contracts and the Reliance on "Off-chain" Resources

Many smart contract-proposed use-cases assume that the smart contract will receive information or parameters from resources that are not on the blockchain itself—so-called off-chain resources. For example, assume a crop insurance smart contract is programmed to transfer value to an insured party if the temperature falls below 32 degrees at any point. The smart contract will need to receive that temperature data from an agreed source. This presents two issues. First, smart contracts do not have the ability to pull data from off-chain resources; rather, that information needs to be "pushed" to the smart contract. Second, if the data at issue is in constant flux, and since the code is replicated across multiple nodes across the network, different nodes may be receiving different information, even just a few seconds apart. In our example, Node-1 may receive information that the temperature is 31.9 degrees, while Node-2 may receive information that the temperature is actually 32 degrees. Given that consensus is required across the nodes for a transaction to be validated, such fluctuations can cause the condition to be deemed "not satisfied."

Contracting parties will be able to solve this conundrum by using a so-called "oracle." Oracles are trusted third parties that retrieve off-chain information and then push that information to the blockchain at predetermined times. In the foregoing example, the oracle would monitor the daily temperature, determine that the freezing event has occurred and then push that information to the smart contract.

Although oracles present an elegant solution to accessing off-chain resources, this process adds another party with whom the parties would need to contract to effectuate a smart contract, thus somewhat diluting the decentralized benefits of smart contracts. It also introduces a potential "point of failure." For example, an oracle might experience a system flaw and be unable to push out the necessary information, provide erroneous data or simply go out of business. Smart contracts will need to account for these eventualities before their adoption can become more widespread.

What is the "Final" Agreement Between the Parties?

When analyzing traditional text-based contracts, courts will examine the final, written document to which the parties have agreed in order to determine whether the parties are in compliance or breach. Courts have long emphasized that it is this final agreement that represents the mutual intent of the parties—the "meeting of the minds."

In the case of code-only smart contracts, the code that is executed—and the outcome it produces—represents the only objective evidence of the terms agreed to by the parties. In these cases, email exchanges between the parties as to what functions the smart contract "should" execute, or oral discussions to that effect, likely would yield to the definitive code lines as the determinative manifestation of the parties' intent.

With respect to ancillary smart contracts, a court likely would look at the text and code as a unified single agreement. The issue becomes complicated when the traditional text agreement and the code do not align. In the crop insurance example described above, assume the text of an agreement specifies that an insurance payout will be made if the temperature falls below 32 degrees, while the smart contract code triggers the payment if the temperature is equal to or below 32 degrees. Assuming that the text agreement does not state whether the text or code controls in the event of an inconsistency, courts will need to determine—perhaps on a case-by-case basis—whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail. In some respects, the analysis should be no different than a case where the provisions of a main agreement differ from what is reflected in an attached schedule or exhibit. The fact that here the conflict would be between text and computer code and not two text documents should not be determinative, but courts may take a different view.

One solution will be for parties to use a text based contract where the parameters that trigger the smart contract execution are not only visible in the text but actually populate the smart contract. In our example, "less than 32 degrees" would not only be seen in the text, but also would create the parameter in the smart contract itself, thereby minimizing the chances of any inconsistency.

The Automated Nature of Smart Contracts

One of the key attributes of smart contracts is their ability to automatically and relentlessly execute transactions without the need for human intervention. However, this automation, and the fact that smart contracts cannot easily be amended or terminated unless the parties incorporate such capabilities during the creation of the smart contract, present some of the greatest challenges facing widespread adoption of smart contracts.

For example, with traditional text contracts, a party can easily excuse a breach simply by not enforcing the available penalties. If a valued customer is late with its payment one month, the vendor can make a real-time decision that preserving the long-term commercial relationship is more important than any available termination right or late fee. However, if this relationship had been reduced to a smart contract, the option not to enforce the agreement on an *ad hoc* basis likely would not exist. A late payment will result in the automatic extraction of a late fee from the customer's account or the suspension of a customer's access to a software program or an internet-connected device if that is what the smart contract was programmed to do. The automated execution provided by smart contracts might therefore not align with the manner in which many businesses operate in the real world.

Similarly, in a text-based contractual relationship, a party may be willing to accept, on an *ad hoc* basis, partial performance to be deemed full performance. This might be because of an interest in preserving a long-term relationship or because a party determines that partial performance is preferable to no performance at all. Here, again, the objectivity required for smart contract code might not reflect the realities of how contracting parties interact.

Amending and Terminating Smart Contracts

At present, there is no simple path to amend a smart contract, creating certain challenges for contracting parties. For example, in a traditional text-based contract, if the parties have mutually agreed to change the parameters of their business deal, or if there is a change in law, the parties quickly can draft an amendment to address that change, or simply alter their course of conduct. Smart contracts currently do not offer such flexibility. Indeed, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain. The result is that amending a smart contract may yield higher transaction costs than amending a text-based contract, and increases the margin of error that the parties will not accurately reflect the modifications they want to make.

Similar challenges exist with respect to terminating a smart contract. Assume a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than it had expected. In a text-based contract, a party can engage in, or threaten, so-called "efficient breach," *i.e.*, knowingly breaching a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe. Moreover, by ceasing performance, or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

Projects are currently underway to create smart contracts that are terminable at any time and more easily amended. While in some ways this is antithetical to the immutable and automated nature of smart contracts, it reflects the fact that smart contracts only will gain commercial acceptance if they reflect the business reality of how contracting parties act.

Objectivity and the Limits of Incorporating Desired Ambiguity Into Smart Contracts

The objectivity and automation required of smart contracts can run contrary to how business parties actually negotiate agreements. During the course of negotiations, parties implicitly engage in a cost-benefit analysis, knowing that at some point there are diminishing returns in trying to think of, and address, every conceivable eventuality. These parties no longer may want to expend management time or legal fees on the negotiations, or may conclude that commencing revenue generating activity under an executed contract outweighs addressing unresolved issues. Instead, they may determine that if an unanticipated event actually occurs, they will figure out a resolution at that time. Similarly, parties may purposefully opt to leave a provision somewhat ambiguous in an agreement in order to give themselves the flexibility to argue that the provision should be interpreted in their favor. This approach to contracting is rendered more difficult with smart contracts where computer code demands an exactitude not found in the negotiation of text-based contracts. A smart contract cannot include ambiguous terms nor can certain potential scenarios be left unaddressed. As a result, parties to smart contracts may find that the transaction costs of negotiating complex smart contracts exceed that of a traditional text-based contracts.

It will take some time for those adopting smart contracts in a particular industry to determine which provisions are sufficiently objective to lend themselves to smart contract execution. As noted, to date, most smart contracts perform relatively simple tasks where the parameters of the "if/then" statements are clear. As smart contracts increase in complexity, parties may disagree on whether a particular contractual provision can be captured through the objectivity that a smart contract demands.

Do Smart Contracts Really Guarantee Payment?

One benefit often touted of smart contracts is that they can automate payment without the need for dunning notices or other collection expenses and without the need to go to court to obtain a judgment mandating payment. While this is indeed true for simpler use cases, it may be less accurate in complex commercial relationships. The reality is that parties are constantly moving funds throughout their organization and do not "park" total amounts that are due on a long-term contract in anticipation of future payment requirements. Similarly, a person obtaining a loan is unlikely to keep the full loan amount in a specified wallet linked to the smart contract. Rather, the borrower will put those funds to use, funding the necessary repayments on an *ad hoc* basis.

If the party owing amounts under the smart contract fails to fund the wallet on a timely basis, a smart contract looking to transfer money from that wallet upon a trigger event may find that the requisite funds are not available. Implementing another layer into the process, such as having the smart contract seek to pull funds from other wallets or having that wallet "fund itself" from other sources, would not solve the problem if those wallets or sources of funds also lack the requisite payment amounts. The parties might seek to address this issue through a text-based requirement that a wallet linked to the smart contract always have a minimum amount, but that solution simply would give the party a stronger legal argument if the dispute was adjudicated. It would not render the payment operation of the smart contract wholly automatic. Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.

Risk Allocation for Attacks and Failures

Smart contracts introduce an additional risk that does not exist in most text-based contractual relationships—the possibility that the contract will be hacked or that the code or protocol simply contains an unintended programming error. Given the relative security of blockchains, these concepts are closely aligned; namely, most "hacks" associated with blockchain technology are really exploitations of an unintended coding error. As with many bugs in computer code, these errors are not glaring, but rather become obvious only once they have been exploited. For example, in 2017 an attacker was able to drain several multi-signature wallets offered by Parity of $31 million in ether. [17] Multi-signature wallets add a layer of security because they require more than one private key to access the wallet. However, in the Parity attack, the attacker was able to exploit a flaw in the Parity code by reinitializing the smart contract and making himself or herself the sole owner of the multi-signature wallets. Parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations are allocated between the parties, and possibly with any third party developers or insurers of the smart contract.

Governing Law and Venue

One of the key promises of blockchain technology, and by extension smart contracts, is the development of robust, decentralized and global platforms. However, global adoption means that parties may be using a smart contract across far more jurisdictions than might exist in the case of text-based contracts. The party offering terms under a smart contract would therefore be best-served by specifying the governing law and venue for that smart contract. A governing law provision specifies what substantive law will apply to the interpretation of the smart contract, whereas a venue clause specifies which jurisdiction's courts will adjudicate the dispute. In cases where governing law or venue is not specified, a plaintiff may be relatively unconstrained in choosing where to file a claim or in arguing which substantive law should apply given the wide range of jurisdictions in which a smart contract might be used. Given that many early disputes concerning smart contracts will be ones of first-impression, contracting parties will want some certainty surrounding where such disputes will be adjudicated.

Best Practices

Given that we are at the nascent stages of smart contract adoption, best practices for implementing such code is still evolving. However, the checklist below should help developers design effective smart contracts and guide companies who

[redacted]

plan to use them.

- For now, parties entering into any type of contractual arrangement would be best served using a hybrid approach that combines text and code. As noted, there are strong arguments that code-only smart contracts should be enforceable, at least under state contract law in the U.S. However, until there is greater clarity on their validity and enforceability, code-only smart contracts should be used only for simpler transactions. Parties will continue to want text-versions of agreements so they can read the agreed-upon terms, memorialize terms that smart contracts are not equipped to address and have a document they know a court will enforce.
- In a hybrid contract using text and code, the text should clearly specify the smart contract code with which it is associated, and the parties should have full visibility into the variables that are being passed to the smart contract, how they are defined and the transaction events that will trigger execution of the code.
- When relying on oracles for off-chain data, the parties should address what would happen if the oracle is unable to push out the necessary data, provides erroneous data or simply goes out of business.
- The parties should consider risk allocation in the event of a coding error.
- The text agreement accompanying the code should specify the governing law and venue, as well as the order of precedence between text and code in the event of a conflict.
- The text agreement should include a representation by each party that they have reviewed the smart contract code, and that it reflects the terms found in the text agreement. Although such a representation cannot force a party to examine the code, it will help the counterparty defend against a claim that the code was never reviewed. Parties may also choose to insure against the risk that the code contains errors. As noted, parties may need to involve third-party experts to review the code.

Future of Smart Contracts

Today, smart contracts are a prototypical example of "Amara's Law," the concept articulated by Stanford University computer scientist Roy Amara that we tend to overestimate new technology in the short run and underestimate it in the long run. Although smart contracts will need to evolve before they are widely adopted for production use in complex commercial relationships, they have the impact to revolutionize the reward and incentive structure that shapes how parties contract in the future. To that end, and when thinking about smart contracts, it is important not to simply think how existing concepts and structures can be ported over to this new technology. Rather, the true revolution of smart contracts will come from entirely new paradigms that we have not yet envisioned.

Endnotes

[1] *See* "What is the 'Gas' in Ethereum?" *Cryptocompare*, November 18, 2016, **available here**.
(go back)

[2] *Id.*
(go back)

[3] Nick Szabo, "Smart Contracts: Building Blocks for Digital Market," 1996, **available here**.
(go back)

[4] Ian Grigg, "The Ricardian Contract," **available here**.
(go back)

[5] *See, e.g.*, "Restatement (Second) of Contracts," Section 1, American Law Institute, 1981. In the U.S., contract law is ordinarily a function of state law. Although this article outlines general contract law principles that are common across states, we note that state law differences may impact the enforceability of smart contracts in certain states.

(go back)

[6] At least one company, AXA, currently offers such a product. **See here**.
(go back)

[7] *See, e.g.*, UCC § 2-201.
(go back)

[8] *See, e.g.*, *Lumhoo v. Home Depot USA, Inc.*, 229 F. Supp. 2d 121, 160 (E.D.N.Y. 2002) (holding that the plaintiffs adduced sufficient evidence to support an inference that the parties formed an oral contract for payment by their employer at an overtime rate for any hours worked in excess of eight hours per day).
(go back)

[9] Uniform Electronic Transactions Act (Unif. Law Comm'n 1999)—New York, Illinois and Washington have state-specific laws relating to the validity of electronic transactions.
(go back)

[10] *Id.* § 2(6).
(go back)

[11] *Id.* § 2 cmt. 5.
(go back)

[12] 15 U.S.C. § 7001(h).
(go back)

[13] 15 U.S.C. § 7006(3).
(go back)

[14] *See* 2017 Ariz. HB 2417 44-7061 and Nev. Rev. Stat. Ann. § 719.090.
(go back)

[15] *See, e.g.*, *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220 (2d Cir. 2016) (reversing the district court's dismissal for failure to state a claim and holding that reasonable minds could disagree as to whether Amazon provided the consumer with reasonable notice of the mandatory arbitration provision at issue).
(go back)

[16] *See* Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, Section 6304 (3d ed. supp. 2011) ("In fact, the exercise of Rule 706 powers is rare under virtually any circumstances. This is, at least in part, owing to the fact that appointing an expert witness increases the burdens of the judge, increases the costs to the parties, and interferes with the adversarial control over the presentation of evidence."), and Stephanie Domitrovich, Mara L. Merino & James T. Richardson, *State Trial Judge Use of Court Appointed Experts: Survey Results and Comparisons*, 50 Jurimetrics J. 371, 373–74 (2010).
(go back)

[17] *See* Haseeb Qureshi, "A Hacker Stole $31M of Ether—How it Happened, and What it Means for Ethereum," *FreeCodeCamp*, (July 20, 2017), **available here**.
(go back)

Both comments and trackbacks are currently closed.

EXHIBIT 202

U.S. DEPARTMENT OF THE TREASURY

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

August 8, 2022

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash, which has been used to launder more than $7 billion worth of virtual currency since its creation in 2019. This includes over $455 million stolen by the Lazarus Group, a Democratic People's Republic of Korea (DPRK) state-sponsored hacking group that was sanctioned by the U.S. in 2019, in the largest known virtual currency heist to date. Tornado Cash was subsequently used to launder more than $96 million of malicious cyber actors' funds derived from the June 24, 2022 Harmony Bridge Heist, and at least $7.8 million from the August 2, 2022 Nomad Heist. Today's action is being taken pursuant to Executive Order (E.O.) 13694, as amended, and follows OFAC's May 6, 2022 designation of virtual currency mixer Blender.io (Blender).

"Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them."

Treasury has worked to expose components of the virtual currency ecosystem, like Tornado Cash and Blender.io, that cybercriminals use to obfuscate the proceeds from illicit cyber activity and other crimes. While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, fraud, and other cybercrimes. Treasury continues to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as foreign partners, to expose, disrupt, and hold accountable perpetrators and persons that enable criminals to profit from cybercrime and other illicit activity. For example, in 2020, Treasury's Financial Crimes Enforcement Network (FinCEN) assessed a $60 million civil money penalty against the owner and operator of a virtual currency mixer for violations of the Bank Secrecy Act (BSA) and its implementing regulations.

MIXER: TORNADO CASH

Tornado Cash (Tornado) is a virtual currency mixer that operates on the Ethereum blockchain and indiscriminately facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin. Tornado receives a variety of transactions and mixes them together before transmitting them to their individual recipients. While the purported purpose is to increase privacy, mixers like Tornado are commonly used by illicit actors to launder funds, especially those stolen during significant heists.

Tornado is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

ILLICIT FINANCE RISKS

Virtual currency mixers that assist criminals are a threat to U.S. national security. Treasury will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financing risks in the virtual currency ecosystem

Criminals have increased their use of anonymity-enhancing technologies, including mixers, to help hide the movement or origin of funds. Additional information on illicit financing risks associated with mixers and other anonymity-enhancing technologies in the virtual asset ecosystem can be found in the 2022 National Money Laundering Risk Assessment .

Those in the virtual currency industry play a critical role in complying with their Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and sanctions obligations to prevent sanctioned persons and other illicit actors from exploiting virtual currency to undermine U.S foreign policy and national security interests. As part of that effort, the industry should take a risk-based approach to assess the risk associated with different virtual currency services, implement measures to mitigate risks, and address the challenges anonymizing features can present to compliance with AML/CFT obligations. As today's action demonstrates, mixers should in general be considered as high-risk by virtual currency firms, which should only process transactions if they have appropriate controls in place to prevent mixers from being used to launder illicit proceeds.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the entity above, Tornado Cash, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, click here.

For identifying information on the entity sanctioned today, as well as associated virtual wallet addresses, click here.

To report a cyber-crime, contact the Federal Bureau of Investigation's Internet Crime Complaint Center here.

For the U.S. government's 2020 DPRK Cyber Threat Advisory, click here.

For information on complying with virtual currency sanctions, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here and OFAC's FAQs on virtual currency here.

###

EXHIBIT 204

Tornado Cash DAO votes to take partial control over treasury funds

theblock.co/post/163274/tornado-cash-dao-votes-to-take-partial-control-over-treasury-funds

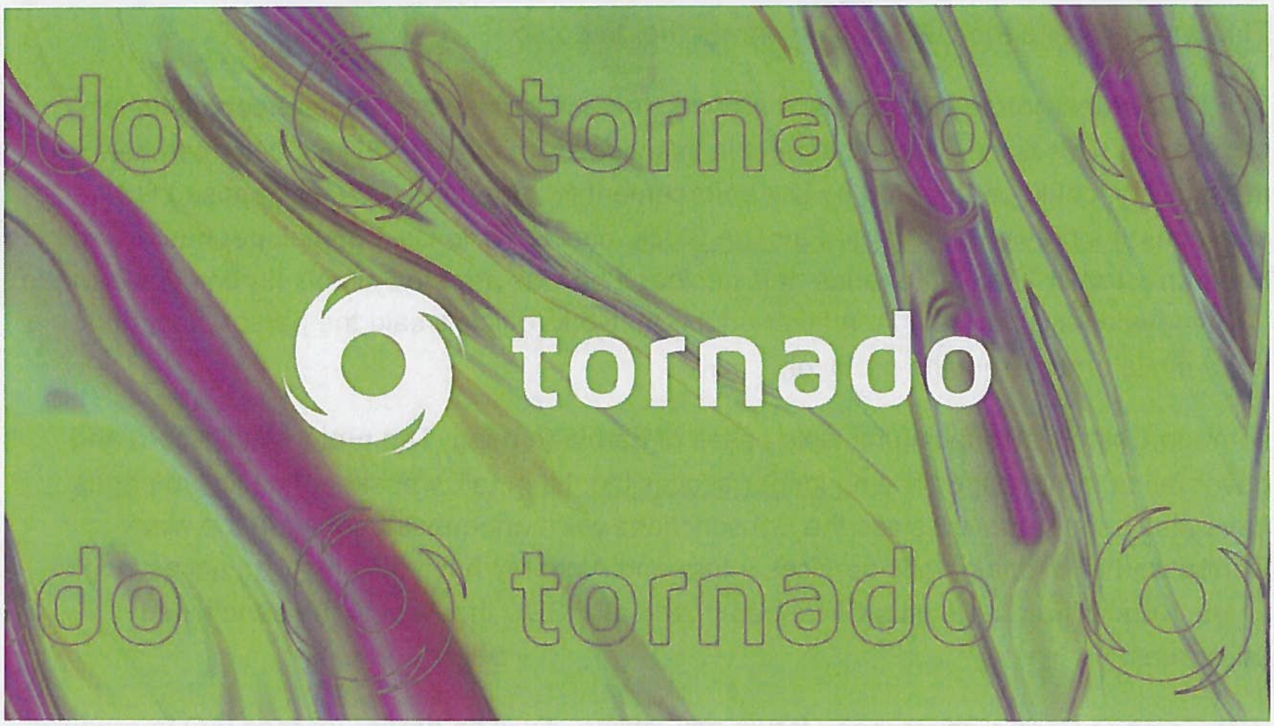
Osato Avan-Nomayo

Governance • August 12, 2022, 10:19AM EDT

The Block

Quick Take

- The Tornado Cash DAO hastily voted to add its own system of governance to the treasury's multisig.
- The DAO's treasury is now controlled by a four-of-six multisig arrangement — with the DAO as one signer.



The Tornado Cash DAO community has voted in favor of adding the DAO's governance as a signatory to the treasury's multi-signatory (multisig) wallet. The treasury looks after about $21.6 million across three different wallets.

This vote began on Wednesday, based on a proposal on the Tornado Cash DAO governance page, and ended today with 100% approval from all 12 participants. These 12 participants contributed 51,000 TORN tokens to push the vote to completion.

The voting process was hastily put together with the SnapShot initiated together with the proposal. Usually, there is a delay between a proposal being filed and the commencement on-chain. This lag is to create adequate time for the community to discuss the matter at hand. But it would have taken too long for the DAO.

"As it is very important, we need to move on fast on this subject. I will make a snapshot vote today so you guys can vote on it during 3 days," said the Tornado Cash DAO member who filed the proposal.

With the vote passed, the DAO's treasury will now become a four-of-six multisig instead of the previous four-of-five multisig arrangement. The Tornado DAO governance will now be added as a signatory to the treasury wallet. Multisig wallets require a specific minimum number of signatories to approve a transaction. In this case, four out of the six signers must approve any transaction from the treasury.

In practice, this means that if the core developers want to make a transaction involving the treasury, they will need to get signatures from at least four of the six multisig holders. Since one of these holders is now the DAO, they may need to ask the DAO to approve a signature.

This would require the DAO to vote on whether to do so.

The DAO's decision to increase its multisig signers is in case something happens to two signatories. This is over fears that people associated with the DAO, including members of the multisig, could be targeted by law enforcement following the recently imposed US sanctions. As previously reported by The Block, one Tornado Cash developer has already been arrested in The Netherlands. It is unclear if he was arrested simply for being a Tornado Cash developer or for being a relayer on the network (officials said the person had made large-scale profits from the protocol).

Tornado Cash is also facing multiple cases of de-platforming. The protocol's Discord and governance forum pages are no longer accessible. Its email, website, and GitHub pages have also been removed since the US sanctions were announced earlier in the week. Centralized blockchain node services Infura and Alchemy have also blocked access to the crypto mixer's front-end, plus Circle has frozen all USDC that was in the sanctioned addresses.

With Tornado Cash's governance forum now offline, it will be harder for the DAO to organize itself and vote on approving any treasury transactions.